A.I. Kostrikin

INTRODUCCIÓN AL ÁLGEBRA

EDITORIAL MIR
MOSCÚ

$$a_0 \quad a_1 \quad \ldots \quad a_n$$
$$a_0 \quad a_1 \quad \ldots \quad a_n$$
$$a_0 \quad a_1 \quad \ldots \quad a_n$$

$$\left(\sum a_i X^i\right) + \left(\sum b_i X^i\right) = \sum (a_i + b_i)$$

$$\left(\sum a_i X^i\right) \cdot \left(\sum b_j X^j\right) = \sum c_k X^k,$$

$$c_k = \sum_{i+j=k} a_i b_j$$

El profesor Alexei Ivanovich Kostrikin, miembro-correspondiente de la Academia de Ciencias de la URSS, laureado con el Premio Estatal, es un destacado matemático. Nació en el año 1929, se graduó en la Universidad de Moscú "Lomonósov" en el año 1952 y en el presente dirige la cátedra de álgebra superior en la misma. Colaborador científico del Instituto de Matemáticas "Steklov" adjunto a la Academia de Ciencias de la URSS. Sus más interesantes investigaciones giran en torno a las álgebras de Lie y sus aplicaciones a los grupos finitos, donde ha logrado valiosos resultados.


ИЗДАТЕЛЬСТВО
МИР

А. И. Кострикин

ВВЕДЕНИЕ В АЛГЕБРУ

Издательство «Наука»

A. I. Kostrikin

INTRODUCCIÓN AL ÁLGEBRA

Traducido del ruso por
Roberto Aníbal Sala,
candidato a doctor en
ciencias económicas

Segunda edición ampliada
y revisada

EDITORIAL MIR · MOSCU

Primera edición. 1978
Segunda edición. 1983

Impreso en la URSS

INDICE

PROLOGO

Este libro está escrito sin ninguna pretensión de originalidad. Su fin es reflejar, en una exposición sistemática, el curso de álgebra conformado y leído, en los últimos años, a los estudiantes de la facultad mecánico-matemática en la Universidad de Moscú. La evolución, completamente natural, de los programas estándares, llevó a la necesidad de modernizar, aunque sea parcialmente, la literatura de estudio sobre el álgebra.

Lamentablemente, el hilo vivo de las lecciones, al exponerse por escrito, se cubrió de tantos detalles y se deformó de tal modo que, involuntariamente, se recuerda una manifestación irónica de Bernard Shaw: «El manual se puede definir como un libro, inservible para la lectura. El hecho de que yo haya resultado un hombre totalmente sin estudio, se lo debo a que nunca pude leer libros de texto, y el tiempo que debiera haber empleado en leer manuales, lo gasté en la lectura de libros auténticos, escritos por personas que realmente saben escribir, lo que jamás ocurre con los autores de manuales» (1933, de una conferencia dada en Hong Kong). Es un débil consuelo, el hecho de que B. Shaw, que pensaba con categorías sumamente paradójicas, no se refería a las matemáticas.

Formalmente, el libro está dividido en dos partes, las cuales, en una primera aproximación, responden a los cursos de álgebra, dictados respectivamente en el primer y tercer semestres. En la parte II, se supone que el lector conoce suficientemente la teoría de espacios vectoriales abstractos y de operadores lineales, cuyo material se estudia en el curso de álgebra lineal y geometría, correspondiente al segundo semestre. Por otra parte, los espacios aritméticos lineales de vectores-filas se exponen en el capítulo 2, una serie de conceptos del álgebra lineal se definen a medida que se avanza en el texto, y un pequeño complemento contiene la teoría geométrica de la reducción de matrices a la forma normal de Jordán. De este modo, el libro se puede estudiar, independientemente de otras fuentes.

Los ejercicios que se encuentran al final de la mayoría de los parágrafos, juegan un importante papel. Existiendo excelentes libros sobre problemas y ejercicios de álgebra*), sería insensato poner acento en los cálculos numéricos, por eso, los ejercicos tienen, preferentemente, carácter teórico y sirven para desarrollar el

---

*) La editorial «Mir» publicó, en 1976, uno de estos libros en español: «Problemas de álgebra superior» de D. Faddiéev e I. Sominski. (N. del T.)

tema principal. En muchos casos, sobre ellos hay referencias en el texto básico, pero, pese a todo, los ejercicios están provistos de indicaciones detalladas para resolverlos. Se recomienda recurrir lo menos posible a estas indicaciones, y en todo caso, después de insistentes pruebas para resolverlos por cuenta propia.

Probablemente, resulte difícil que una cantidad tan modesta de horas lectivas, sea suficiente para abarcar el contenido de todo el libro. Esto, especialmente se refiere a la parte II, cuyo material, por su carácter, no puede considerarse tradicional. Este material proporciona suficiente pábulo a la intuición, pero, algunas «exquisiteces» (como, por ejemplo, el teorema de Silov, invariantes de los grupos lineales, las representaciones de un grupo de rotaciones, o de álgebras no asociativas) están conscientemente dirigidas a los aficionados, como base para ejercicios complementarios.

Por lo visto, una vez estudiado el capítulo 7, bastante difícil, hay que orientarse bien sea hacia los elementos de la teoría de representaciones (capítulo 8), o hacia la teoría general de anillos, módulos y campos, parcialmente tratada en el capítulo 9 (no nos fue posible profundizar en cuestiones estructurales). La primera variante parece preferible, no sólo por su orientación geométrica y su proximidad al curso del segundo semestre, sino también, porque el conocimiento de los principales hechos sobre la teoría de representaciones es muy útil a los matemáticos que, no necesariamente, se especializan en álgebra. Sería sumamente deseable que la idea sobre representaciones de grupos, expresada en el libro mediante un material concreto muy limitado, se consolide con un curso especial de mayor contenido. Como ejemplos de temas aproximados, se pueden citar la teoría de Galois; los grupos engendrados por aplicaciones, incluidos los grupos cristalográficos; las representaciones de los grupos compactos, etc. Por otro lado, el capítulo 9, debido a su orientación teórico-numérica, responde, en mayor medida, a los planes de estudios existentes. Cualquiera sea la variante que se elija, pondrá los fundamentos para seguir estudiando álgebra*).

Aquí hay que advertir con precisión una circunstancia no tan evidente para el estudiante de primer curso. El curso de álgebra superior pese a su nombre, de ningún modo refleja la diversidad del álgebra moderna. Precisamente a eso debe su nombre el libro: introducción al álgebra. Un objetivo más de esta introducción, consiste en suministrar conceptos y resultados necesarios para otros cursos de matemáticas. Sólo se comprende cuan importante es el estudio del lenguaje algebraico, cuando se intenta prescindir de él al estudiar particularmente matemáticas.

Pese a su carácter elemental, el curso tradicional de álgebra, presenta determinadas dificultades para asimilarlo, debido al aspecto

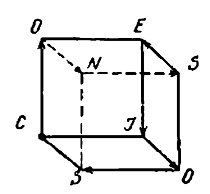
*) Una pequeña lista de literatura complementaria que no pretende ser completa, se da al principio de cada una de las partes del libro.

formal en el razonamiento, que él impone. El autor tuvo constantemente esto en cuenta, tratando de subrayar los vínculos existentes entre el álgebra y otras ramas de las matemáticas. Debemos lamentar, el haber dejado fuera de los límites de este libro elementos sobre la teoría de categorías y de sistemas parcialmente ordenados. Pero, nos pareció totalmente irrazonable transformar el curso introductorio en un conglomerado de conceptos abstractos, provistos de antemano sin saber para que, mermando así el interés hacia el objeto de estudio, debido a su exposición superficial.

Muchas de las variantes ideadas para un curso obligatorio de álgebra, limitado y orientado por el programa estándar «se ensayaron» en la facultad mecánico-matemática de la Universidad de Moscú Lomonósov. Cabe esperar, que esta obra en forma de libro, de una de las últimas variantes del curso, resulte útil para estudiantes, graduados y profesores de otros institutos de enseñanza superior, así como para aquellas personas que se inician, por su cuenta, en el estudio del álgebra. Por supuesto, el orden y la plenitud expositiva del material del libro en las lecciones del curso, dependerán considerablemente de la situación concreta y de las tradiciones en la enseñanza.

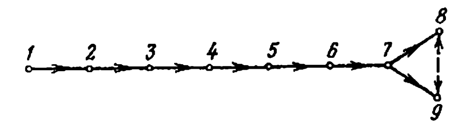
El autor expresa su profunda gratitud al experto colectivo de docentes de la cátedra de álgebra superior de la Universidad de Moscú, y también a quienes proporcionaron útiles consejos sobre la exposición del curso. Todas las ulteriores proposiciones constructivas, así como informaciones y observaciones de errores u omisiones, se recibirán con gran reconocimiento.

A. Kostrikin



AL LECTOR

De acuerdo al plan general, expuesto en el prólogo, el esquema de la dependencia de los capítulos tiene la siguiente forma:



(la flecha punteada muestra una dependencia débil). Se comprende que al lector experimentado (digamos, docente o estudiante de segundo curso) no le será difícil comenzar la lectura, prácticamente desde cualquier lugar, naturalmente, si está dispuesto a dirigirse, de tiempo en tiempo, a las definiciones en parágrafos y capítulos anteriores. No todos los nuevos conceptos se introducen en los párrafos que comienzan con la palabra «definición». Un índice detallado y el índice de materias ayudan a encontrar el lugar necesario en el libro.

Cada capítulo está dividido en varios parágrafos, y cada parágrafo en varios puntos, con sus propios títulos. Dentro del parágrafo los teoremas, proposiciones, lemas, corolarios, tienen su numeración propia: teorema 1, teorema 2, . . .; lema 1, lema 2, . . . Con esta numeración primitiva, pero muy evidente y económica, cuando se hacen citas sobre afirmaciones de otro parágrafo, se precisa escribir teorema i del § j, o incluso teorema i del § j del cap. k, sin embargo, esto no crea incomodidades.

El final de una demostración (o en su ausencia) se anota con el signo ∎.

Para abreviar, se usan símbolos lógicos elementales. El signo de implicación $\Rightarrow$ en la escritura $A \Rightarrow B$ tiene la sencilla carga significativa, que «A trae consigo a B», o que «de A sigue B», al mismo tiempo, que «$A \rightleftharpoons B$» significa la equivalencia de las enunciaciones A y B (... si, y sólo si, ...). El cuantificador universal $\forall$ reemplaza la expresión «para todo». Las restantes designaciones son comprensibles del contexto.

Abajo se escribe la totalidad del alfabeto griego, con indicación de las pronunciaciones de las letras. La confusión que a veces se observa aquí es lamentable, por cuanto las letras del alfabeto griego son muy empleadas en matemáticas.

ALFABETO GRIEGO

Αα	Ββ	Γγ	Δδ	Εε	Ζζ
Alfa	Beta	Gamma	Delta	Epsilon	Zeta
Ηη	Θθ	Ιι	Κκ	Λλ	Μμ
Eta	Theta	Iota	Kappa	Lambda	My
Νν	Ξξ	Οο	Ππ	Ρρ	Σσ
Ny	Xi	Omicron	Pi	Rho	Sigma
Ττ	ϑ	Φφ	Χχ	Ψψ	Ωω
Tau	Ipsilon	Fi	Ji	Psi	Omega

«El álgebra es generosa, frecuentemente da más de lo que le piden»
(*D'Alembert*)

Parte I

FUNDAMENTOS DEL ALGEBRA

Esta parte se puede considerar álgebra en miniatura. Los conceptos fundamentales de grupo, anillo, campo, a los que el estudiante novel no está acostumbrado, se introducen, en la medida de lo posible, informalmente y en dosis mínimas, pese a lo cual, el número de conceptos derivados resulta bastante grande. No es necesario memorizarlos: resultarán habituales cuando el estudiante, por su propia cuenta, trabaje sobre los problemas y ejercicios. Para comodidad, se destacan algunos de los sistemas algebraicos más usados (los grupos $(\mathbb{Z}+)$, S_nA_n, $GL(n)$, $SL(n)$; anillo de los polinomios; campos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y Z_p), que sirven, además, para mostrar el lenguaje del álgebra. Por tradición y por consideraciones de sucesión entre la escuela y la universidad, inicialmente se expone la técnica de matrices y determinantes, empleada para buscar e investigar resoluciones de sistemas de ecuaciones lineales. En este camino, naturalmente, surgen las estructuras algebraicas fundamentales.

LITERATURA COMPLEMENTARIA

1. *Van der Waerden B. L.*, Álgebra, «Nauka», 1976, (en ruso).
2. *I. M. Vinogradov*, Fundamentos de la teoría de números, «Nauka», 1972, (en ruso).
3. *G. Devienport*, Aritmética superior, «Nauka», 1965, (en ruso).
4. *A. G. Kurosch*, Curso de Álgebra superior, «Mir», 1977, (en español).
5. *Lang S.*, Álgebra, «Mir» 1968, (en inglés).
6. *Proskuriakov I. V.*, Problemas de álgebra lineal, «Nauka», 1974, (en ruso).
7. *Faddiéev D.*, *Sominski I.*, Problemas de álgebra superior, «Mir», 1977, (en español).

Capítulo 1

FUENTES DEL ALGEBRA

¿Dónde comienza el álgebra? Con cierta aproximación se puede decir, que las fuentes del álgebra se hallan en el arte de sumar, multiplicar y elevar a potencia números enteros. El reemplazo de números por letras, hecho formal pero no siempre evidente y de significado único, permite operar con reglas análogas en los límites de sistemas algebraicos más generales. O sea, el intento de dar una respuesta completa a la cuestión planteada, no sólo nos llevaría a lejanos siglos, a los secretos del germen del pensamiento matemático. La parte más difícil de la respuesta estaría ligada a la descripción de las estructuras algebraicas de nuestros días: grupos, anillos, campos, módulos, etc. Pero a esto precisamente se dedica todo el libro, así que por ahora el objetivo del capítulo 1 parece inalcanzable.

Felizmente, debajo de la envoltura abstracta de la mayoría de las teorías axiomáticas del álgebra se ocultan problemas concretos de carácter teórico o práctico, cuyas resoluciones sirvieron en su tiempo para generalizaciones felices, y a veces dieron lugar a conclusiones de largo alcance. Por otra parte, una teoría desarrollada daba impulso y medios para la solución de nuevos problemas. La compleja interrelación de los aspectos teóricos y aplicados de la teoría, común a toda la matemática, en el álgebra se rezuma con gran claridad y, en alguna medida, justifica el estilo concéntrico de exposición adoptado por nosotros.

Luego de unas breves observaciones generales, relacionadas con la historia de esta disciplina, formularemos algunos problemas que anticipan el contenido de los capítulos siguientes. Uno de estos problemas servirá como punto de partida para el estudio de sistemas de ecuaciones lineales, teoría de matrices y de determinantes. Desarrollaremos el método de Gauss y obtendremos los primeros conocimientos acerca de las resoluciones de sistemas lineales.

Ya en esta etapa es útil introducir terminología y notación unificadas, para lo que daremos una revista concisa a la teoría de conjuntos y de aplicaciones.

Serán introducidos conceptos fundamentales de relación de equivalencia y de factorización de las aplicaciones. Más adelante, en relación con el esclarecimiento del principio de inducción matemática, se establecerán proporciones combinatorias elementales. Finalmente, las propiedades aritméticas más simples del sistema de números enteros, citados en el último parágrafo, no sólo se utilizan

ulteriormente, sino que sirven de prototipo para la construcción de una aritmética análoga en sistemas algebraicos más complejos.
El material de este capítulo no va mucho más allá de los límites del programa escolar. Del lector se requiere solamente su disposición para asumir un punto de vista un poco más general. Se puede comenzar la lectura desde el § 3

§ 1. ALGEBRA BREVE

En nuestros días, no sin fundamento, se habla sobre la «algebraización» de las matemáticas, o sea sobre la penetración de ideas y métodos del álgebra en las partes teórica y aplicada de las matemáticas. Este estado de cosas, totalmente claro ya a mediados del siglo XX, de ningún modo se observó siempre. Como cualquier otro campo de la actividad humana, las matemáticas están expuestas a la influencia de la moda. La moda de los métodos algebraicos es provocada por la esencia de las cosas, aunque debido a su atracción a veces se franquean las fronteras de lo razonable. Y como la envoltura algebraica, que obscurece el contenido, no es menor desgracia que un elemental olvido del álgebra, entonces no es casual que el mérito de uno u otro libro ya depende (muy razonablemente) de la habilidad del autor de evitar una sobrecarga de formalismo algebraico.
Si dejamos aparte los extremos, entonces al álgebra desde la antigüedad constituía una parte esencial de las matemáticas. Lo mismo habría que decir sobre la geometría, pero nos resguardaremos tras una frase alada de Sofía Germain (siglo XIX): «El álgebra no es otra cosa que la geometría escrita en símbolos, y la geometría es sencillamente álgebra expresada en figuras». Desde entonces la situación ha cambiado, pero parece que «es reconocido que la «naturaleza» de los objetos matemáticos es, en esencia, un hecho secundario y que es poco importante, por ejemplo, si presentamos los resultados en forma de teorema de geometría «pura» o con ayuda de la geometría analítica en forma de teorema algebraico» (N. Bourbaki).
En correspondencia con el principio de que «no son importantes los objetos matemáticos, sino las relaciones entre ellos» el álgebra se define (un poco tautológicamente y en forma absolutamente incomprensible para el profano) como ciencia acerca de las operaciones algebraicas, efectuadas sobre los elementos de diferentes conjuntos. Las propias operaciones algebraicas surgieron de la aritmética elemental. A su vez, en base a las reflexiones algebraicas se obtienen las demostraciones más naturales de muchos hechos de la «aritmética superior», o sea de la teoría de los números.
Pero el significado de las estructuras-conjuntos con las operaciones algebraicas lejos sobrepasa el marco de las aplicaciones teóri-

co-numéricas. Muchos objetos matemáticos (espacios topológicos, ecuaciones diferenciales, funciones de variables múltiples complejas, etc.) se estudian mediante la construcción de las debidas estructuras algebraicas, aunque no sean adecuadas a los objetos estudiados en todo caso, reflejan sus aspectos esenciales. Algo semejante se refiere a los objetos del mundo real.

Un juicio preciso sobre esto fue formulado hace más de 45 años atrás por uno de los creadores de la mecánica cuántica P. Dirac «...La física moderna requiere una matemática más abstracta y el desarrollo de sus fundamentos. Así, la geometría no-euclidiana y el álgebra no conmutativa, consideradas en un tiempo como sencillamente fruto de la imaginación o producto de reflexiones lógicas ahora son reconocidas como muy necesarias para la descripción de cuadro general del mundo físico».

Los medios algebraicos son muy útiles al investigar las partículas elementales en la mecánica cuántica, las propiedades del cuerpo rígido y cristales (en relación con esto especialmente importante es la teoría de representación de grupos), al analizar modelos económicos, al construir modernas máquinas computadoras, etc.

A su vez, el álgebra se nutre de los jugos vivificantes de otras disciplinas, incluidas las matemáticas. Así, por ejemplo, los métodos homológicos del álgebra surgieron de las entrañas de la topología y de la teoría algebraica de números.

Por eso no sorprende que los rasgos del álgebra y los puntos de vista sobre ésta cambiaron en distintas épocas. No tenemos posibilidad de seguir detalladamente esos cambios no sólo por falta de espacio, sino principalmente porque la descripción sobre la historia de la asignatura debe ser concreta, exigencia que puede ser satisfecha solamente con un conocimiento fundamental de la misma.

Nos limitaremos a una enumeración esquemática de nombres y períodos.

Civilizaciones antiguas de Babilonia y Egipto. Civilización griega. «Aritmética» de Diofante (siglo III).	Operaciones aritméticas sobre conjuntos de números enteros y racionales positivos. Fórmulas algebraicas en cálculos astronómicos y geométricos. Formulación de problemas de construcciones (sobre la duplicación del cubo y trisección del ángulo), que se ocuparon los algebristas mucho más tarde.
Civilización oriental del medioevo. Escritos del nativo de Jiva Muhammad b Musa al-Jwarizmi (aprox. año 825) «Kitab al-mujtasar min hisab al-yabr wa-l-muqabala».	Ecuaciones algebraicas de primer y segundo grados. Aparición del propio vocablo «álgebra».
Epoca del Renacimiento.	Resolución de ecuaciones algebraicas de tercero y cuarto grado.

Fibonacci (Leonardo de Pisa) (aprox.	1170-1250)	
S. Ferro	(1465-1526)	
N. Tartaglia	(1500-1557)	
J. Cardán	(1501-1576)	
L. Ferrari	(1522-1565)	
F. Viete	(1540-1603)	Elaboración de la simbólica algebraica moderna.
R. Bombelli	(1530-1572)	
Siglos XVII y XVIII		
R. Descartes	(1596-1650)	Aparición de la geometría analítica, puente sólido entre la geometría y el álgebra. Animación de la actividad en la teoría de números. Desarrollo del álgebra de polinomios. Búsqueda intensiva de fórmulas generales para la resolución de ecuaciones algebraicas. Primeros accesos a la demostración de la existencia de raíces en una ecuación con coeficientes numéricos. Principios de la teoría de determinantes.
P. Fermat	(1601-1665)	
I. Newton	(1646-1727)	
G. Léibniz	(1646-1716)	
L. Euler	(1707-1783)	
J. D'Alembert	(1717-1783)	
J. L. Lagrange	(1736-1813)	
G. Cramer	(1704-1752)	
P. Laplace	(1749-1827)	
Vandermonde	(1735-1796)	
Siglo XIX y principio del siglo XX		
C. F. Gauss	(1777-1855)	Demostración del teorema fundamental de existencia de raíces en las ecuaciones con coeficientes numéricos. Desarrollo intensivo de la teoría de números algebraicos.
P. Dirichlet	(1805-1859)	
E. Kummer	(1810-1893)	
L. Kronecker	(1823-1891)	
R. Dedekind	(1831-1916)	
E. I. Zolotariov	(1847-1878)	
G. F. Voronoi	(1868-1908)	
A. A. Márkov	(1856-1922)	
P. L. Chébychev	(1821-1894)	Búsqueda de métodos de resolución aproximada de las ecuaciones algebraicas. Condiciones de los coeficientes que aseguran una disposición dada de las raíces.
C. Hermite	(1822-1901)	
N. I. Lobachevsky	(1792-1856)	
A. Hurwitz	(1859-1919)	
A. Ruffini	(1765-1822)	Demostración de la imposibilidad en caso general, de resolver ecuaciones de grado $n \geqslant 5$ en radicales. Desarrollo de funciones algebraicas. Formulación de la teoría de Galois. Principios sobre la teoría de grupos finitos, preferentemente en base a grupos permutables.
N. E. Abel	(1802-1829)	
C. Jacobi	(1804-1851)	
E. Galois	(1811-1832)	
B. Riemann	(1826-1866)	
B. Cauchy	(1789-1857)	
C. Jordan	(1838-1922)	
L. Sílov	(1832-1918)	
G. Grassmann	(1809-1877)	Desarrollo intensivo de los métodos de álgebra lineal.
D. Sylvester	(1814-1897)	
A. Cayley	(1821-1895)	
W. Hámilton	(1805-1865)	Aparición de los sistemas hipercomplejos, luego del descubrimiento de los cuaterniones (estos sistemas ahora se denominan álgebras). En particular, en relación con el desarrollo de los grupos continuos (grupos de Lie), fueron colocados los fundamentos del álgebra de Lie. Se desarrolla-
J. Boole	(1815-1864)	
S. Lie	(1842-1899)	
G. Frobenius	(1849-1918)	
J. Serret	(1819-1885)	
M. Noether	(1844-1922)	
D. A. Grave	(1863-1939)	
A. Pioncaré	(1854-1912)	

F. Klein (1849-1925)
W. Burnside (1852-1927)
J. Schur (1885-1941)
H. Weyl (1885-1955)
F. Enríquez (1871-1946)
J. Von Neumann (1903-1957)
D. Hilbert (1862-1943)
E. Cartán (1869-1951)
C. Guénzel (1861-1941)
E. Stéinitz (1871-1928)
E. Noether (1882-1935)
E. Artin (1898-1962)
J. Birkhoff (1884-1947)
N. Bourbaki «Elementos de matemática».

ron la geometría algebraica y la teoría de invariantes como partes importantes de las matemáticas. En el siglo XIX la matemática aún no había alcanzado una diferenciación sutil y muchos grandes sabios trabajaban creativamente en varios de sus campos.
La primera mitad del siglo XX fue distinguida por una reconstrucción fundamental de todo el edificio de la matemática. El álgebra, renunciando al privilegio de ser la ciencia sobre ecuaciones algebraicas, resueltamente se planteó sobre un camino de desarrollo axiomático y mucho más abstracto.

Se hizo de uso corriente el lenguaje de las teorías de anillos, módulos, categorías, homología. Muchas teorías dispersas hallaron cabida en el esquema general del álgebra universal. En el punto de enlace del álgebra con la lógica matemática nació la teoría de modelos. Las viejas teorías se renovaron, ensanchando sus campos de aplicación. Como ejemplos pueden servir la geometría algebraica moderna, la topología algebraica, la K-teoría algebraica, la teoría de grupos algebraicos. Algunos despegues brillantes experimentó la teoría de grupos finitos.

Toda el álgebra se encuentra ahora en una situación de desarrollo dinámico. En esto, grandes méritos les caben a los matemáticos soviéticos. El elevado nivel de las investigaciones alcanzado en nuestro país en mucho se debe a científicos tales como N. G. Chebotariov (1894-1947), O. Yu. Schmidt (1891-1956), A. Y. Máltsev (1909-1967), A. G. Kurosch (1908-1971), P. S. Nóvikov (1901-1975).

§ 2. ALGUNOS PROBLEMAS MODELO

Los cuatro problemas formulados más abajo son de distinto nivel. Los primeros tres, que por sí mismos no son equivalentes, están exclusivamente destinados para motivar la investigación de campos de diferentes tipos, espacios lineales, grupos y sus presentaciones, o sea de aquellas teorías algebraicas que serán tratadas más adelante. Las «soluciones» de estos problemas han sido expuestas en muchas monografías especiales. El cuarto problema, que anticipa el estudio de los sistemas lineales, es útil tratar de resolverlo inmediatamente, antes de pasar al parágrafo siguiente, donde se aportan los razonamientos necesarios.

1. Problema sobre la resolución de ecuaciones en radicales. Del álgebra elemental es conocida la fórmula

$$x_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a} \qquad (1)$$

para las soluciones x_1, x_2 de la ecuación cuadrática ax^2+bx+ $+c=0$.

La ecuación de tercer grado $x^3 + ax^2 + bx + c = 0$ reemplazando $x \mapsto x - \frac{1}{3}a$ se lleva a la forma $x^3 + px + c = 0$. Esta ecuación reducida siempre tiene tres raíces x_1, x_2, x_3. Si se hace

$$D = -4p^3 - 27q^2, \qquad \varepsilon = \frac{-1+\sqrt{-3}}{2},$$

$$u = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}, \quad v = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}} \qquad (2)$$

(las raíces cúbicas se eligen de tal modo, que $uv = -3p$), entonces se puede demostrar que

$$x_1 = \frac{1}{3}(u+v), \quad x_2 = \frac{1}{3}(\varepsilon^2 u + \varepsilon v), \quad x_3 = \frac{1}{3}(\varepsilon u + \varepsilon^2 v). \qquad (3)$$

Las expresiones (2) y (3) se denominan fórmulas de Cardán (1545) y se las asocian también con los nombres de otros matemáticos italianos de la época del Renacimiento (S. Ferro, N. Tartaglia), al igual que la fórmula (1), son válidas para cualesquiera coeficientes a, b, c, p, q, que puede tomar, por ejemplo, un valor racional arbitrario. Fórmulas análogas fueron halladas para las raíces de las ecuaciones de cuarto grado y en el transcurso de casi trescientos años se hicieron intentos infructuosos de «resolver en radicales» la ecuación general de quinto grado. Sólo en 1813 A. Ruffini (en una primera aproximación) y en el año 1827 N. Abel (independientemente y en forma rigurosa) demostraron el teorema acerca de que la ecuación en el caso general $x^n + a_1x^{n-1} + \ldots + a_n = 0$ cuando $n > 4$ no tiene solución en radicales. Un descubrimiento fundamental en este campo fué efectuado por Evaristo Galois en 1831, cuando éste tenía sólo veinte años (este trabajo fue conocido recién en 1846) y formuló un criterio universal para resolver en radicales no sólo la ecuación general de grado n sino cualquiera (por ejemplo, con coeficientes racionales).

A cada polinomio (ecuación) de grado n él le confrontó un campo de descomposición y una familia finita de automorfismos de este campo (con potencia no mayor de $n!$), ahora denominado grupo Galois del campo (o del polinomio original). Aunque no tenemos posibilidad de detenernos más detalladamente en la teoría de Galois, en el capítulo 7 será destacada por sus propiedades puramente internas, una clase especial de los denominados grupos resolubles. Resulta, que la ecuación de grado n con coeficientes racionales tiene solución exacta en radicales, cuando tiene solución el grupo de Galois que le es correspondiente. Sea, por ejemplo, dada la ecuación de quinto grado $x^5 - ax - 1 = 0$, donde a es un número entero cualquiera. A este número responde el grupo de Galois G_a, dependiente de algún modo complejo de a. G_0 es un grupo cíclico de orden 4 (siendo, por definición, resolubles todos los grupos cíclicos) y la

ecuación $x^5 - 1 = 0$, sin duda, se resuelve en radicales. Por el contrario, G_1 tiene la misma estructura que el grupo simétrico S_5 de orden 120 y este último, como se muestra en el capítulo 7, es insoluble. Por lo tanto, no tiene solución en radicales la ecuación $x^5 - x - 1 = 0$.

Observemos finalmente, que para las necesidades prácticas, la posibilidad de expresar las raices de las ecuaciones algebraicas en forma explícita por medio de radicales, no tiene crucial importancia; son más actuales los diferentes métodos de cálculo aproximado de las raíces. Pero este hecho no disminuye la belleza del éxito de Galois, quien con sus ideas influyó poderosamente en el desarrollo posterior de las matemáticas. Para comenzar, precisamente Galois formuló las bases de la teoría de los grupos. La correspondencia recíproca univalente entre los subcampos del campo de descomposición y los subgrupos de su grupo, establecida por Galois, se enriqueció en el siglo XX con nuevas construcciones abstractas y se constituyó en un medio irreemplazable de investigación de objetos matemáticos.

2. Problema sobre los estados de una molécula poliatómica. Cada molécula se puede considerar como un sistema de partículas, núcleos atómicos (rodeados de electrones). Si en el momento inicial de tiempo la configuración del sistema es cercana a la de equilibrio, entonces, en determinadas condiciones, las partículas integrantes del sistema siempre se quedarán cerca de la situación de equilibrio y no alcanzarán grandes velocidades. Los movimientos de este tipo se denominan oscilaciones respecto a una configuración equilibrada, y el sistema se llama estable. Es sabido que cualquier oscilación pequeña de una molécula, cerca de la situación de equilibrio estable, es superposición de las llamadas oscilaciones normales. En muchos casos se logra determinar la energía potencial de la molécula y sus frecuencias normales, tomando en cuenta la simetría interior de la molécula. La simetría de la estructura molecular se describe por medio de un grupo puntual de una molécula. Las distintas realizaciones de este grupo finito (sus representaciones irreducibles) y la relación con estas realizaciones de la función en el grupo (caracteres de la representación), determinan los parámetros de las oscilaciones de la molécula.

Por ejemplo, a la molécula de agua H_2O (fig. 1) le corresponde el grupo cuaternario de Klein (producto directo de dos grupos cíclicos de segundo orden), y a la molécula de fósforo P_4 (fig. 2), que tiene la forma de tetraedro regular en cuyos vértices se disponen los átomos del fósforo, le corresponde el grupo simétrico S_4 de orden 24. Las representaciones irreducibles de estos grupos serán estudiadas en el cap. 8. En la actualidad el desarrollo de la teoría estructural de las moléculas resulta difícil concebirlo sin la ayuda de la teoría de grupos.

Una aplicación mucho más temprana de la teoría de grupos se relaciona con la cristalografía. Ya en el año 1891 el eminente cristalógrafo ruso E. S. Feódorov, y luego el sabio alemán A. Schoenflies, hallaron 230 grupos cristalográficos espaciales, que describen todas las simetrías de cristales existentes en la naturaleza. Desde entonces, la teoría de grupos se usa permanentemente para la investi-

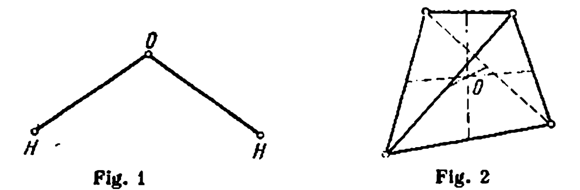


Fig. 1 Fig. 2

gación de la influencia de la simetría sobre las propiedades físicas de los cristales.

3. Problema de la codificación de las comunicaciones. En la construcción de sistemas automáticos de comunicaciones, terrestres o cósmicos, frecuentemente, en calidad de comunicación elemental se toma una sucesión—fila (o palabra) ordenada $a = (a_1, a_2, \ldots$ $\ldots, a_n)$ de longitud n, donde $a_i = 0$ ó 1. Como las operaciones comunes de suma y multiplicación por módulo 2, se prestan muy bien para su cumplimiento en máquinas electrónicas, y los propios símbolos 0 y 1 son cómodos para la transmisión en forma de señales eléctricas (1 y 0 se distinguen por las fases de las señales divididas en el tiempo, o por sus existencia o ausencia), entonces, no sorprende que el campo GF (2) (véase § 4, cap. 4), resulte un atributo necesario para el especialista en elaboración de información. A veces es cómodo usar en calidad de a_i los elementos de otros campos finitos.

Con el fin de excluir la influencia de interferencia (cargas atmosféricas, ruidos cósmicos, etc.), capaces de transformar los 0 en 1 y viceversa, se requiere tomar a a lo suficientemente larga y utilizar un sistema especial de *codificación*, o sea elegir un subconjunto (*código*) S_0 de filas (palabras en código) transmitidas de todo el conjunto S de las mismas, tal que sea posible restablecer a por medio de la palabra alterada recibida a', a condición de que no tengan lugar demasiados errores. Así aparecen los *códigos correctores de errores*. La teoría algebraica de codificación, ampliamente desarrollada en los últimos años y que propuso métodos muy ingeniosos de codificación, básicamente tiene que ver con códigos lineales especiales, cuando la elección de S_0 está vinculada con la construcción de matrices rectangulares especiales y con la resolución de sistemas de ecuaciones lineales, cuyos coeficientes pertenecen al

campo finito dado. Un ejemplo sencillo de tal código será mostrado en el cap. 5.

4. Problema de la lámina caliente. Una lámina rectangular plana con tres perforaciones (fig. 3) es usada en calidad de válvula en un dispositivo imaginario para la obtención de bajas temperaturas. En la válvula se ha marcado una redecilla (parrilla) cuadrada. Sus vértices situados en los cuatro contornos se denominan limítrofes,

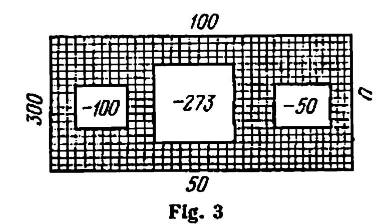


Fig. 3

y los restantes vértices internos. Una medición inmediata muestra que, ante cualquier calentamiento o enfriamiento, la temperatura de cada vértice interior resulta ser la media aritmética de las temperaturas de los cuatro vértices más próximos, sean éstos limítrofes o internos. Se espera que las piezas del dispositivo, al estar en contacto con distintas partes de los contornos, comuniquen a los correspondientes puntos limítrofes las temperaturas indicadas en la fig. 3. ¿Acaso es posible esto?, y si es posible, ¿resultará simple la distribución de la temperatura en los puntos interiores?

§ 3. SISTEMAS DE ECUACIONES LINEALES. PRIMEROS PASOS

Las ecuaciones lineales $ax = b$ y los sistemas del tipo

$$\begin{aligned} ax + by &= e \\ cx + dy &= f \end{aligned} \tag{1}$$

con coeficientes reales a, b, c, d, e, f «se resuelven» en la escuela secundaria. Nuestra tarea es aprender a operar con *un sistema de ecuaciones algebraicas lineales* (o sintéticamente: con un sistema lineal) de la forma más general

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m. \end{aligned} \tag{2}$$

Aquí m y n son números enteros positivos (naturales) arbitrarios. Aunque el paso de (1) a (2) parezca sólo una complicación cuanti-

tativa, en realidad, de hecho, tiene una importancia capital. Los sistemas del tipo (2) se hallan en toda la matemática, y los llamados métodos lineales, cuyo producto final frecuentemente son las soluciones de sistemas lineales, componen su parte más desarrollada. Es suficiente recordar, que la teoría de los sistemas de tipo (2) sirvió a fines del siglo XIX como prototipo para la creación de la teoría de ecuaciones integrales, que juegan un papel sumamente importante en la mecánica y en la física. La resolución de un gran número de problemas en las máquinas computadoras también se reducen a sistemas del tipo (2).

1. Terminología. Es preciso prestar atención al significado muy económico y cómodo de los coeficientes del sistema (2): *el coeficiente* a_{ij} (se lee a-i-jota; por ejemplo: a_{12} es a-uno-dos, y de ningún modo a-doce) corresponde a la i-ésima ecuación y a la j-ésima *incógnita* x_j. El número b_i se denomina *término independiente* de la i-ésima ecuación. El sistema (2) se llama *homogéneo*, si $b_i = 0$ para $i = 1, 2, \ldots$ $\ldots, m$. Cualquier b_i sistema lineal

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= 0, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ &\cdot\ \cdot \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= 0 \end{aligned} \tag{2'}$$

se llama *sistema homogéneo, asociado* al sistema (2), o también sistema *reducido* del (2).

Los coeficientes de las incógnitas componen la tabla rectangular

$$\left\| \begin{matrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \cdot & \cdot & \cdot\ \cdot\ \cdot & \cdot \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{matrix} \right\| \tag{3}$$

llamada *matriz de dimensiones* $m \times n$ (matriz m por n, o matriz cuadrada de orden n cuando $m = n$) y en forma abreviada denotada por el símbolo (a_{ij}) o sencillamente con la letra A. Naturalmente, se habla de la i-ésima fila $(a_{i1}, a_{i2}, \ldots, a_{in})$ de la matriz (3) y de la j-ésima columna

$$\left\| \begin{matrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{matrix} \right\|$$

que en adelante, para economizar espacio, se designará como una fila, encerrada entre corchetes $[a_{1j}, a_{2j}, \ldots, a_{mj}]$. En el caso de una matriz cuadrada se habla también de *la diagonal principal*, compuesta por los elementos $a_{11}, a_{22}, \ldots, a_{nn}$. La matriz (a_{ij}) que tiene todos sus elementos nulos, excepto los de su diagonal prin-

cipal, se escribe a veces con el símbolo diag $(a_{11}, a_{22}, \ldots, a_{nn})$ y se llama matriz *diagonal*, y cuando $a_{11} = a_{22} = \ldots = a_{nn} = a$, se denota con el símbolo $\mathrm{diag}_n\,(a)$ y se denomina matriz *escalar*. Para indicar la matriz $\mathrm{diag}_n\,(1)$, llamada matriz *unidad* de orden n, frecuentemente se usa el símbolo E_n o la letra E, si es que la dimensión de la matriz está dada.

Junto con la matriz (3) se examina también la matriz *ampliada* $(a_{ij} \mid b_i)$ del sistema (2), obtenida de (3) con el agregado de la columna $[b_1, b_2, \ldots, b_m]$ los términos independientes; para mayor claridad separada del resto de las columnas por una línea vertical.

Si cada una de las ecuaciones del sistema (2) se transforma en una identidad luego de sustituir las incógnitas x_i por los números x_i°, entonces, el conjunto de n números $x_1^\circ, x_2^\circ, \ldots, x_n^\circ$ se llama *solución* del sistema (2), y x_i° es el i-ésimo *componente de la solución*. Se dice también que el conjunto $x_1^\circ, x_2^\circ, \ldots, x_n^\circ$ satisface todas las ecuaciones del sistema (2). El sistema que no tiene solución alguna, se llama *incompatible*. Si el sistema tiene soluciones, se llama *compatible*, y si la solución es única, *determinado*. Puede existir más de una solución: entonces se dice que el sistema es *indeterminado*. Es o no compatible un sistema dado de ecuaciones lineales, y si lo es, cuáles son todas sus soluciones; éstas son las cuestiones inmediatas, a las que se deben dar respuestas.

Veamos otra vez el problema del punto 4 del § 2. Numeramos todos los puntos internos de la plancha, en forma arbitraria, del 1 al 416 (número preciso de ellos que hay en la fig. 3), agreguémosle 204 números de puntos limítrofes y, de acuerdo con la regla dada para el cálculo de la temperatura t_i en el punto interior que lleva el número i, formamos 416 relaciones del tipo

$$t_e = \frac{t_a + t_b + t_c + t_d}{4}$$

Sea, digamos, $a, b, c \leqslant 416$, y $d > 416$. Entonces esta relación se puede volver a escribir en forma de ecuación lineal

$$-t_a - t_b - t_c + 4t_e = t_d$$

con el miembro $t_d = -273, -100, -50, 0, 50, 100$ ó 300 (siendo posibles otras variantes). Tomadas conjuntamente, estas ecuaciones conforman el sistema lineal cuadrado de tipo (2) con $n = m = 416$. Los coeficientes de las incógnitas t_i son iguales a 0 (la mayoría), -1 ó 4. ¿Es este sistema compatible y determinado? Nosotros obtuvimos una formulación distinta, matemáticamente exacta, de un problema de carácter cualitativo. La cuestión sobre la existencia y la unicidad es sumamente típica para muchas ramas de la matemática, relacionadas con el estudio de los fenómenos físicos.

2. Equivalencia de sistemas lineales. Sea dado un sistema lineal «de las mismas dimensiones»

$$\begin{matrix} a'_{11}x_1 + a'_{12}x_2 + \ldots + a'_{1n}x_n = b'_1 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a'_{m1}x_1 + a'_{m2}x_2 + \ldots + a'_{mn}x_n = b'_m. \end{matrix} \qquad (2')$$

Decimos, que el sistema (2') es obtenido del (2) con ayuda de *una transformación elemental del tipo* (I), si en el sistema (2) todas las ecuaciones, excepto la i-ésima y k-ésima, quedaron como antes, y estas dos ecuaciones se intercambiaron de lugar. Si en (2') todas las ecuaciones, excepto la i-ésima, son las mismas que en (2), y la i-ésima ecuación de (2') tiene la forma

$$(a_{i1} + ca_{k1})\, x_1 + \ldots + (a_{in} + ca_{kn})\, x_n = b_i + cb_k \qquad (*)$$

donde c es un número cualquiera (o sea, $a'_{ij} = a_{ij} + ca_{kj}$, $b'_i = b_i + cb_k$), entonces suponemos que el sistema (2) ha sufrido *una transformación elemental del tipo* (II).

Los sistemas lineales (2) y (2') se llaman *equivalentes*, si ambos son simultáneamente incompatibles, o bien son compatibles y tienen las mismas soluciones.

Conviniendo en indicar la equivalencia de los sistemas (a) y (b) con el símbolo $(a) \sim (b)$, observamos que $(a) \sim (a)$, de $(a) \sim (b)$ sigue que $(b) \sim (a)$, y de $(a) \sim (b)$ y $(b) \sim (c)$ resulta que $(a) \sim (c)$.

Un indicio suficiente de equivalencia de sistemas se contiene en la siguiente afirmación.

TEOREMA 1. *Dos sistemas lineales son equivalentes, si uno se obtiene del otro aplicando una sucesión finita de transformaciones elementales.*

Es suficiente demostrar la equivalencia de los sistemas (2) y (2'), obtenido de (2), al aplicar una transformación elemental. Observemos, que el sistema (2) se obtiene del (2') también como resultado de una transformación elemental, por cuanto estas transformaciones son invertibles. En otras palabras, en el caso (I), cambiando otra vez de lugar a las ecuaciones i y k, regresamos al sistema inicial; análogamente, en el caso de tipo (II), sumando a la i-ésima ecuación en (2'), la k-ésima, multiplicada por ($-c$), obtendremos la i-ésima ecuación del sistema (2).

Demostremos ahora, que cualquier solución $(x_1^\circ, \ldots, x_n^\circ)$ del sistema (2) resulta también solución del sistema (2'). Si fue realizada una transformación elemental del tipo (I), entonces, las propias ecuaciones, en general, no cambiaron (sólo cambió el orden de sus inscripciones). Por eso, los números $x_1^\circ, x_2^\circ, \ldots, x_n^\circ$, que antes las satisfacían, las satisfacerán luego de la transformación. En el caso de una transformación elemental del tipo (II), las ecuaciones, excepto la i-ésima, no se modificaron, y por eso la solución $(x_1^\circ, x_2^\circ, \ldots, x_n^\circ)$ satisface a éstas como antes. En lo que concierne a la i-ésima ecua-

ción, ella adoptó la forma (∗). Tal como nuestra solución satisface las i-ésima y k-ésima ecuaciones del sistema (2), entonces

$$a_{i1}x_1^\circ + \ldots + a_{in}x_n^\circ = b_i, \quad a_{k1}x_1^\circ + \ldots + a_{kn}x_n^\circ = b_k.$$

Multiplicando ambas partes de la última identidad por c, y sumando esto a la primera, obtenemos, agrupando los miembros, una identidad del tipo (∗) con $x_i = x_i^\circ$.

En virtud de la reversibilidad de las transformaciones elementales, observada arriba, las reflexiones realizadas demuestran también que, recíprocamente, cualquier solución del sistema (2′) será solución del sistema (2).

Queda observar, que la incompatibilidad de un sistema proporciona la incompatibilidad del otro (demostración por el contrario). ∎

3. Reducción a la forma escalonada. Por medio de una aplicación sucesiva de transformaciones elementales se puede pasar de un sistema de ecuaciones dado, a otro sistema de forma más simple.

Primero, señalemos, que entre los coeficientes a_{i1} se tiene por lo menos uno, distinto de cero. En caso contrario no tendría sentido mencionar la incógnita x_1. Si $a_{11} = 0$, intercambiamos de lugar la primera ecuación y cualquier otra j-ésima, tal que $a_{j1} \neq 0$ (o sea, transformación de tipo (I)). Ahora el coeficiente de la primera incógnita en la primera ecuación es distinto de cero. Lo indicamos por medio de a'_{11}. Restemos de la i-ésima ecuación ($i = 2, 3, \ldots, m$) del nuevo sistema, la primera ecuación multiplicada por un coeficiente c_i tal, que luego de la resta el coeficiente de x_1 se anule ($m - 1$ transformaciones elementales del tipo (II)). Es evidente, que para ello es necesario tomar $c_i = a_{i1}/a'_{11}$. Como resultado, obtendremos un sistema en el cual x_1 entra sólo en la primera ecuación. También puede suceder que la segunda incógnita no figure en todas las ecuaciones con número $i > 1$. Sea x_k la incógnita con el menor número, que integra cualquier ecuación, excepto la primera. Obtendremos el sistema

$$\begin{aligned}
a'_{11}x_1 + \ldots + a'_{1n}x_n &= b'_1,\\
a'_{2k}x_k + \ldots + a'_{2n}x_n &= b'_2,\\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ &\\
a'_{mk}x_k + \ldots + a'_{mn}x_n &= b'_m, \quad k > 1, \quad a'_{11} \neq 0.
\end{aligned}$$

No prestando ahora atención a la primera ecuación, aplicamos el procedimiento anterior a las restantes. Después de una serie de transformaciones elementales, el sistema inicial toma la forma

$$\begin{aligned}
a''_{11}x_1 + \ldots\ldots\ldots + a'_{1n}x_n &= b''_1,\\
a''_{2k}x_k + \ldots\ldots + a''_{2n}x_n &= b''_2,\\
a''_{3l}x_l + \ldots + a''_{3n}x_n &= b''_3,\\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ &
\end{aligned}$$

$$a''_{ml}x_l + \ldots + a''_{mn}x_n = b''_m, \quad 1 > k > 1, \quad a''_{11} \neq 0, \quad a''_{2k} \neq 0.\}$$

Por supuesto, aquí $a''_{1j} = a'_{1j}$, $b''_1 = b'_1$, ya que la primera ecuación no fue alterada.

Seguimos adoptando este procedimiento mientras sea posible. Es claro que deberemos detenernos cuando se hagan nulos no sólo el coeficiente de la incógnita de turno (digamos la s-ésima), sino y los coeficientes de todas las incógnitas siguientes, hasta la n-ésima. Finalmente, el sistema (2) tomará la forma

$$\begin{aligned} a_{11}x_1 + \ldots\ldots\ldots\ldots + \bar{a}_{1n}x_n &= \bar{b}_1, \\ \bar{a}_{2k}x_k \ldots\ldots\ldots + \bar{a}_{2n}x_n &= \bar{b}_2, \\ \bar{a}_{3l}x_l \ldots\ldots + \bar{a}_{3n}x_n &= \bar{b}_3, \\ \ldots\ldots\ldots\ldots\ldots & \\ \bar{a}_{rs}x_s \ldots + \bar{a}_{rn}x_n &= \bar{b}_r, \\ 0 &= \bar{b}_{r+1} \\ 0 &= \bar{b}_m. \end{aligned} \tag{4}$$

Aquí $\bar{a}_{11}\bar{a}_{2k}\bar{a}_{3l} \ldots \bar{a}_{rs} \neq 0$, $1 < k < l < \ldots < s$. Puede suceder que $r = m$ y por eso, ecuaciones del tipo $0 = \bar{b}_t$ en el sistema (4) no habrán. Se dice que el sistema de ecuaciones del tipo (4) tiene forma *escalonada*.

Este nombre no es adoptado por todos: se puede hablar de forma *trapezoidal* o de forma *cuasitriangular*, etc., pero esto no es esencial.

TEOREMA 2. *Cualquier sistema de ecuaciones lineales es equivalente al sistema de forma escalonada.*

La demostración se deduce inmediatamente de los razonamientos anteriores. ▮

A veces resulta más cómodo efectuar las transformaciones elementales no sobre el sistema, sino sobre su matriz ampliada $(a_{ij} \mid b_i)$. Del mismo modo que el teorema 2, se demuestra el

TEOREMA 2'. *Cualquier matriz puede llevarse a la forma escalonada, con la ayuda de transformaciones elementales.* ▮

4. Investigación de un sistema de ecuaciones lineales. Las cuestiones de compatibilidad y determinación, en virtud de los teoremas 1 y 2, es suficiente investigarlas para los sistemas de forma escalonada (4).

Comencemos con la cuestión de la compatibilidad. Es evidente, que si el sistema (4) contiene ecuaciones del tipo $0 = \bar{b}_t$, con $\bar{b}_t \neq 0$, entonces, este sistema es incompatible, puesto que la igualdad $0 = \bar{b}_t$ no puede ser satisfecha por ningún valor para las incógnitas. Demostremos, que si en el sistema (4) no hay tales ecuaciones, entonces el sistema es compatible.

Y bien, sea $\bar{b}_t = 0$ para $t > r$. Llamaremos incógnitas *principales* a $x_1, x_k, x_l, \ldots, x_s$, con las cuales comienzan la primera, segunda, ..., y r-ésima ecuaciones, respectivamente; las restantes incógnitas, si es que las hay, se denominan *independientes*. Por definición, sólo hay r incógnitas principales.

Otorgamos a las incógnitas independientes valores arbitrarios, y los sustituimos en el sistema (4). Entonces, para x_s se obtiene una ecuación de (r-ésima) tipo $ax_s = b$, con $a = \bar{a}_{rs} \neq 0$, la cual tiene solución única. Sustituyendo el valor obtenido $x_s = x_s^\circ$ en las primeras $r - 1$ ecuaciones, y yendo por el sistema (4) de abajo arriba, nos convencemos de que los valores de las incógnitas principales se determinan unívocamente para cualquier valor que se dé a las incógnitas independientes. Hemos demostrado

TEOREMA 3. *Para la compatibilidad de un sistema de ecuaciones lineales es necesario y suficiente que, después de ser reducido a la forma escalonada, en él no se encuentren ecuaciones del tipo* $0 = \bar{b}_t$, con $\bar{b}_t \neq 0$. *Si esta condición se cumple, entonces, a las incógnitas independientes se les pueden dar valores arbitrarios; las incógnitas principales (con valores dados a las independientes) se determinan unívocamente en el sistema.* ∎

Aclaremos ahora, cuándo el sistema será determinado, suponiendo que se cumple la condición de compatibilidad establecida por nosotros. Si en el sistema (4) hay incógnitas independientes, entonces el sistema a ciencia cierta es indeterminado: podemos otorgar a las incógnitas independientes cualquier valor, expresando por medio de ellas las incógnitas principales (por teorema 3). Pero si no hay incógnitas independientes y, por lo visto, todas son principales, entonces, de acuerdo al teorema 3, ellas se determinan del sistema unívocamente, o sea el sistema resulta determinado. Queda por observar, que la ausencia de incógnitas independientes equivale a la condición $r = n$. Nosotros hemos demostrado la siguiente afirmación.

TEOREMA 4. *El sistema lineal compatible* (2) *es determinado si y sólo si, en el sistema escalonado* (4) *obtenido de él, se cumple la igualdad* $r = n$. ∎

Si $m = n$, un sistema lineal, reducido a la forma escalonada, puede expresarse también así (*forma triangular*):

$$\begin{aligned} \bar{a}_{11}x_1 + \bar{a}_{12}x_2 + \ldots + \bar{a}_{1n}x_n &= \bar{b}_1, \\ \bar{a}_{22}x_2 + \ldots + \bar{a}_{2n}x_n &= \bar{b}_2, \\ \cdots\cdots\cdots\cdots\cdots & \\ \bar{a}_{nn}x_n &= \bar{b}_n, \end{aligned} \qquad (5)$$

si se descuida el cumplimiento de la condición $\bar{a}_{ij} \neq 0$ para todas las i. Efectivamente, la inscripción (5) significa, que en el sistema.

la k-ésima ecuación no contiene incógnitas x_i con $i < k$, y esta condición es a todas luces cumplida para los sistemas del tipo escalonado.

Observemos, para el futuro, que la matriz (a_{ij}) con elementos $a_{ij} = 0$ para todo $i > j$ se llama *triangular superior*. Análogamente se define la matriz *triangular inferior*.

De los teoremas 3 y 4 se deduce

COROLARIO 1. *Cuando* $m = n$ *el sistema lineal* (2) *es compatible y determinado si, y sólo si, luego de ser reducido a la forma escalonada, se obtiene el sistema* (5) *con* $\bar{a}_{11}\bar{a}_{22} \ldots \bar{a}_{nn} \neq 0$. ∎

Prestemos atención al hecho, de que esta condición no depende de los términos independientes del sistema. Por eso, si $m = n$ el sistema (2) es compatible y determinado si y sólo si, ello es cierto para el sistema homogéneo (2′), asociado al (2). Pero un sistema homogéneo siempre es compatible: ya que tiene, por ejemplo, la solución nula $x_1^\circ = 0, \ldots, x_n^\circ = 0$.

La condición $\bar{a}_{11}\bar{a}_{22} \ldots \bar{a}_{nn} \neq 0$ significa que el sistema homogéneo posee sólo solución nula. Llegamos a otra forma de corolario 1, no vinculada con su forma escalonada.

COROLARIO 1. *El sistema lineal* (2), *siendo* $m = n$ *es compatible y determinado si y sólo si, su sistema asociado homogéneo* (2′) *sólo tiene solución nula.* ∎

Una atención especial se merece el caso cuando $n > m$.

COROLARIO 2. *El sistema compatible* (2) *con* $n > m$ *es indeterminado. En particular, el sistema homogéneo con* $n > m$ *siempre tiene solución no nula.*

Efectivamente, en todo caso $r \leqslant m$, por cuanto en el sistema (4) no hay más ecuaciones que en el sistema (2) (las ecuaciones con identidades iguales a cero para ambos miembros, son desechadas). Por eso, la desigualdad $n > m$ lleva a $n > r$, lo que, de acuerdo al teorema 4, significa indeterminación del sistema (2). Queda por observar, que la indeterminación de un sistema homogéneo, equivale a la existencia de una solución no nula del mismo. ∎

Parte de los resultados obtenidos se reflejan en la tabla siguiente.

	Forma del sistema lineal			
	General	Homogénea	$n > m$ no homogénea	$n > m$ homogénea
Número de soluciones	0, 1, ∞	1, ∞	0, ∞	∞

5. Observaciones particulares y ejemplos. El método expuesto por nosotros para resolver un sistema de ecuaciones lineales se llama *método de Gauss* o *método de eliminación consecutiva de las incógnitas.*

Sumamente cómodo cuando n no es muy grande, también sirve para ser realizado en computadoras, aunque, por distintas razones, con frecuencia otros modos de resolución resultan más prácticos, por ejemplo, los métodos iterativos. Esto especialmente se refiere al caso en que los coeficientes son dados, y la solución se busca con un determinado grado de exactitud. En las investigaciones teóricas, sin embargo, una importancia primordial adquieren la formulación de las condiciones de compatibilidad o de determinación de los sistemas lineales, y también la búsqueda y el hallazgo de fórmulas generales para encontrar los valores de los coeficientes y de los términos independientes, sin reducir el sistema a la forma escalonada. En alguna medida, a una de estas exigencias da respuesta el corolario 1'.

EJEMPLO 1. Volvemos otra vez al problema de la plancha caliente, formulado en el § 2. Como vimos en el punto 1, la cuestión que nos ocupa se expresa con propiedad por medio de un sistema lineal muy concreto (para definirlo, lo llamaremos PC) con un número considerablemente grande de incógnitas t_i. Siguiendo el criterio formulado en el corolario 1', consideremos el sistema lineal homogéneo HPC, asociado al PC. En otras palabras, la temperatura en todos los puntos limítrofes, se toma igual a cero. Sea e el número del punto interior con el mayor valor $|t_e|$. Entonces, de la condición

$$t_e = \frac{t_a + t_b + t_c + t_d}{4}$$

se deduce que $|t_e| = |t_a| = |t_b| = |t_c| = |t_d|$. Moviéndonos a un paso de la parilla en cualquiera de las 4 direcciones, pasaremos por puntos de idéntico valor $|t_i| = |t_e|$, hasta que no alcancemos un punto limítrofe con temperatura nula. O sea, $|t_e| = 0$, y por eso, también $t_i = 0$, para todas las i. Y bien, el sistema HPC tiene solamente solución nula, y, por lo visto, PC es un sistema lineal compatible y determinado. De este modo, el problema de la plancha caliente, en su formulación inicial, queda resuelto.

EJEMPLO 2. Dado el sistema lineal

$$\begin{aligned} &x_1 \ldots\ldots\ldots\ldots\ldots\ldots = 1,\\ &x_2 \ldots\ldots\ldots\ldots\ldots\ldots = 1,\\ &-x_1 - x_2 + x_3 \ldots\ldots\ldots\ldots = 0,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &\qquad -x_{n-2} - x_{n-1} + x_n = 0. \end{aligned}$$

Es evidente, que este es un sistema compatible y determinado, reducido a la forma escalonada (triangular). Sólo que, al resolverlo, es necesario avanzar de arriba abajo y no de abajo arriba. Por definición, la solución se llama sucesión de los primeros n números de *Fibonacci* $f_1, f_2, \ldots, f_n$. Estos números están vinculados a un fenómeno botánico, denominado filotaxis (disposición de las hojas en el tallo). Sin embargo, cuando $n = 1000$ o aún con n arbitrario, se desearía indicar la expresión general (fórmula analítica) para el enésimo número de Fibonacci. El lector puede replicar, argumentando que también le alcanza la paciencia para indicar y f_{1000} siguiendo la definición inductiva de estos números. Pero, esto no será una solución matemática de la cuestión. En los capítulos 2 y 3 indicaremos dos expresiones para f_n, aunque, por cierto, este problema concreto puede resolverse con medios más directos.

OBSERVACION. A veces resulta más cómodo resolver un sistema lineal, sin reducirlo a la forma escalonada. Esto especialmente se refiere al caso cuando la matriz del sistema contiene muchos ceros. Un poco de práctica es aquí preferible a largas explicaciones.

§ 4. DETERMINANTES DE ORDENES PEQUEÑOS

Al exponer el método de Gauss, no nos preocupamos demasiado acerca de los valores de los coeficientes de las incógnitas principales. Era solamente importante que estos coeficientes fueran distintos de cero. Llevaremos a cabo ahora un proceso más cuidadoso de eliminación de incógnitas, aunque sea en el caso de sistemas lineales cuadrados de pequeñas dimensiones. Esto nos dará sustento para las reflexiones y materia prima para la construcción de una teoría general de los determinantes en el capítulo 3.

Como en el § 3, consideremos un sistema de dos ecuaciones con dos incógnitas

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 &= b_1, \\ a_{31}x_1 + a_{22}x_2 &= b_2 \end{aligned} \qquad (1)$$

y tratemos de hallar una fórmula general para los componentes de su solución, x y x_2. Denominemos *determinante* de la matriz

$$\begin{Vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{Vmatrix}$$

a la expresión $a_{11}a_{22}-a_{21}a_{12}$ y designémoslo con el símbolo $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$. Asimismo, a la matriz cuadrada se le confronta el número

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{12}-a_{21}a_{22}. \qquad (2)$$

Si tratamos de eliminar a x_2 del sistema (1), multiplicando la primera ecuación por a_{22}, y sumando a esto la segunda ecuación multiplicada por $-a_{12}$, entonces obtenemos

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} x_1 = b_1a_{22}-b_2a_{12}.$$

El segundo miembro se puede considerar como el determinante de la matriz $\begin{Vmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{Vmatrix}$. Supongamos que $\begin{Vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{Vmatrix} \neq 0$. Entonces tenemos

$$x_1 = \frac{\begin{vmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}} \quad \text{y análogamente} \quad x_2 = \frac{\begin{vmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{22} \end{vmatrix}}. \qquad (3)$$

Teniendo las fórmulas para la resolución de un sistema de dos ecuaciones lineales con dos incógnitas, podemos resolver algunos otros sistemas (resolver sistemas = encontrar sus soluciones). Examinemos, por ejemplo, un sistema de dos ecuaciones homogéneas con tres incógnitas:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= 0, \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= 0. \end{aligned} \qquad (4)$$

Nos interesa una solución no nula de este sistema, en la cual, por consiguiente, por lo menos una de las $x_i \neq 0$. Sea, por ejemplo, $x_3 \neq 0$. Dividiendo ambas partes por $-x_3$ y haciendo $y_1 = -x_1/x_3$, $y_2 = -x_2/x_3$, escribimos el sistema (4) en la misma forma:

$$\begin{aligned} a_{11}y_1 + a_{12}y_2 &= a_{13}, \\ a_{21}y_1 + a_{22}y_2 &= a_{23}, \end{aligned}$$

que el (1). Con el supuesto de que $\begin{vmatrix} a_{13} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0$, las formulas (3) dan

$$y_1 = -\frac{x_1}{x_3} = \frac{\begin{vmatrix} a_{13} & a_{12} \\ a_{23} & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}, \quad y_2 = -\frac{x_2}{x_3} = \frac{\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}.$$

No es sorprendente, que del sistema (4) determinamos no las propias x_1, x_2, x_3, sino que solamente sus relaciones: de la homogeneidad del sistema se deduce fácilmente que, si (x_1^0, x_2^0, x_3^0) es solución y c es un número cualquiera, entonces (cx_1^0, cx_2^0, cx_3^0) también será solución. Por eso, podemos hacer

$$x_1 = -\begin{vmatrix} a_{13} & a_{12} \\ a_{23} & a_{22} \end{vmatrix}, \quad x_2 = -\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix}, \quad x_3 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \qquad (5)$$

y decir, que cualquier solución se obtiene de la indicada, multiplicando todas las x_i por algún número c. Para darle a la respuesta una forma más simétrica, observemos que siempre

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = -\begin{vmatrix} b & a \\ d & c \end{vmatrix},$$

tal como se observa inmediatamente de la fórmula (2). Por eso las (5) se puede anotar así

$$x_1 = \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}, \quad x_2 = -\begin{vmatrix} a_{12} & a_{13} \\ a_{21} & a_{23} \end{vmatrix}, \quad x_3 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}. \qquad (6)$$

Estas fórmulas se dedujeron suponiendo que $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0$. No es difícil probar, que la aseveración demostrada es cierta, si por lo menos uno de los determinantes que integran la expresión (6)

es distinto de cero. Si los tres determinantes son nulos, entonces, por supuesto, las fórmulas de (6) dan una solución (precisamente, nula), pero no podemos afirmar que todas las soluciones se obtienen de ella, multiplicando por un número (examine el sistema compuesto de dos ecuaciones coincidentes $x_1 + x_2 + x_3 = 0$).

Pasemos ahora al caso de tres ecuaciones con tres incógnitas:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= b_1, \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= b_2, \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 &= b_3. \end{aligned}$$

Queremos eliminar de este sistema x_2 y x_3, para obtener el significado de x_1. Con este fin multiplicamos la primera ecuación por c_1, la segunda por c_2, la tercera por c_3, y las sumamos. Elegimos c_1, c_2, c_3 de tal modo, que en la ecuación obtenida, los términos que contienen x_2 y x_3 se anulen. Igualando a cero los coeficientes correspondientes, obtenemos para c_1, c_2 y c_3 el sistema de ecuaciones

$$\begin{aligned} a_{12}c_1 + a_{22}c_2 + a_{32}c_3 &= 0, \\ a_{13}c_1 + a_{23}c_2 + a_{33}c_3 &= 0, \end{aligned}$$

del mismo tipo que el (4). Por eso se puede tomar

$$c_1 = \begin{vmatrix} a_{22} & a_{32} \\ a_{23} & a_{33} \end{vmatrix}, \quad c_2 = -\begin{vmatrix} a_{12} & a_{32} \\ a_{13} & a_{33} \end{vmatrix}, \quad c_3 = \begin{vmatrix} a_{12} & a_{22} \\ a_{13} & a_{23} \end{vmatrix}.$$

Luego de cambios evidentes, obtenemos para x_1 la expresión

$$\left(a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{23} \end{vmatrix} - a_{21}\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}\right)x_1 =$$

$$= b_1\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - b_2\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + b_3\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}. \quad (7)$$

El coeficiente de x_1 se llama determinante de la matriz

$$\begin{Vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{Vmatrix} \quad \text{y se anota} \quad \begin{Vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{Vmatrix}.$$

De este modo, como determinante de tercer orden, tomamos la expresión

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{21}\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} =$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}, \quad (8)$$

dada con ayuda de determinantes de segundo orden. Es fácil observar, que el segundo miembro de la igualdad (7) se obtiene del coeficiente de x_1 sustituyendo a_{11} por b_1, a_{21} por b_2 y a_{31} por b_3. Por eso la igualdad (7) se puede escribir de la forma siguiente

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} x_1 = \begin{vmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{vmatrix}$$

Supongamos que el coeficiente de x_1 es distinto de cero. Entonces, efectuando cálculos análogos para x_2 y x_3, llegamos a las fórmulas

$$x_1 = \frac{\begin{vmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}}, \quad x_2 = \frac{\begin{vmatrix} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}}, \quad x_3 = \frac{\begin{vmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}} \qquad (9)$$

Es evidente, que los mismos razonamientos son aplicables a un sistema de cuatro, cinco y más ecuaciones, con el mismo número de incógnitas. Para esto, necesitamos primeramente deducir fórmulas análogas a (6) para resolver un sistema homogéneo de tres ecuaciones con cuatro incógnitas; luego en el sistema de cuatro ecuaciones con cuatro incógnitas excluir x_2, x_3, x_4, multiplicando las ecuaciones por c_1, c_2, c_3, c_4, sumándolas a continuación. Hallaremos los valores de c_i ($i = 1, 2, 3, 4$) para el sistema de tres ecuaciones homogéneas.

El coeficiente, obtenido para x_1 y compuesto de determinantes de tercer orden de forma (8), se denomina determinante de cuarto orden. Siguiendo los mismos razonamientos para x_2, x_3, x_4, hallamos para las x_i fórmulas análogas a (9). Así se puede continuar ilimitadamente. La certeza de que en algún momento llegaremos a la meta, nos la da un principio general, ampliamente usado en las matemáticas, precisamente, el principio de inducción matemática (véase el § 7).

EJERCICIOS

1. La fórmula (8) es más fácil de recordar, si usamos la regla práctica de los signos para la escritura de los productos, que integran el desarrollo del determinante de tercer orden (fig. 4). Hallar una regla análoga para el determinante de cuarto orden.

2. Mostrar que los seis términos de la descomposición del determinante de tercer orden no pueden ser conjuntamente positivos.

3. El cuadrado de la superficie de un paralelogramo, construido por los radios-vectores de puntos P, Q con coordenadas cartesianas (α, β) y (γ, δ)

(fig. 5), se expresa con la fórmula

$$\Delta^2=\begin{vmatrix} \alpha^2+\beta^2 & \alpha\gamma+\beta\delta \\ \alpha\gamma+\beta\delta & \gamma^2+\delta^2 \end{vmatrix}.$$

Es particularmente fácil convencerse de esto, si se usa un sistema de coordenadas tal, que el punto P quede situado en el eje Ox. Hallar una fórmula aná-

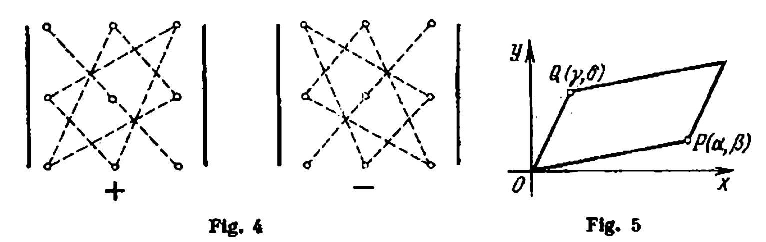


Fig. 4 Fig. 5

loga para el cuadrado del volumen de un paralelepípedo en el espacio tridimensional, usando el determinante de tercer orden.

§ 5. CONJUNTOS Y APLICACIONES

En los dos parágrafos precedentes nos encontramos con conjuntos de elementos de distinta naturaleza, al igual que con las aplicaciones de conjuntos. El conjunto de soluciones de un sistema de ecuaciones lineales dado, o la regla que coloca en correspondencia con cada matriz de segundo orden a su determinante, resultan sólo manifestaciones particulares de ese círculo de conceptos formales, cuyo conocimiento, aunque sea a un nivel intuitivo, es útil para el futuro.

1. Conjuntos. Se entiende por conjunto una agrupación en un todo de objetos, denominados a su vez *elementos* del primero. Los conjuntos con un número finito de distintos elementos pueden ser circunscriptos por medio de una evidente enumeración de todos sus elementos; por lo común estos elementos se encierran entre llaves. Por ejemplo, $\{1, 2, 4, 8\}$ es un conjunto de potencias de dos, encerradas entre 1 y 10. Como regla, el conjunto se designa con una letra mayúscula de algún alfabeto, y sus elementos con letras minúsculas del mismo o de otro alfabeto. Para los conjuntos más importantes, se adoptan notaciones uniformes, que conviene observar. Así, las letras $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ correspondientemente significan conjuntos de los números positivos enteros (naturales), de todos los números enteros, de los números racionales, y de los números reales. Para un conjunto S dado, *la notación* $a \in S$ indica que a es un elemento perteneciente al conjunto S; en caso contrario se escribe $a \notin S$. Se dice que S es un *subconjunto* del conjunto T o $S \subset T$ (T contiene a S), cuando tiene lugar la implicación

$$x \in S, \quad \forall x \Rightarrow x \in T.$$

(Con respecto a las notaciones, véase la parte «al lector», pag. 13). Dos conjuntos S y T coinciden (o son iguales) si ambos contienen los mismos elementos. Simbólicamente:

$$S = T \Leftrightarrow S \subset T \quad \text{y} \quad T \subset S$$

($\Leftrightarrow$ significa «si y sólo si» o «atrae a ambos lados»). *El conjunto vacío* $\varnothing$, que no contiene ningún elemento, por definición integra el número de subconjuntos de cualquier conjunto. Si $S \subset T$, pero $S \neq \varnothing$ y $S \neq T$, entonces S es un subconjunto propio en T. Para la distinción del subconjunto $S \subset T$ frecuentemente usan alguna propiedad inherente sólo a los elementos de S. Por ejemplo,

$$\{n \in \mathbb{Z} \mid n = 2m \quad \text{para algún} \quad m \in \mathbb{Z}\}$$

es el conjunto de todos los números enteros pares, y

$$\mathbb{N} = \{n \in \mathbb{Z} \mid n > 0\}$$

es el conjunto de los números naturales.

Se entiende como *intersección* de dos conjuntos S y T, al conjunto

$$S \cap T = \{x \mid x \in S \quad \text{y} \quad x \in T\},$$

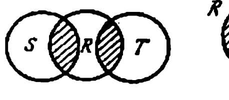
y, por su *unión* (o reunión), al conjunto

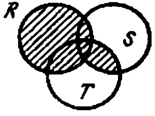
$$S \cup T = \{x \mid x \in S \quad \text{o} \quad x \in T\}.$$

La intersección de $S \cap T$ puede ser un conjunto vacío. Entonces se dice que *S y T* son conjuntos *disjuntos.* Las operaciones de intersección y unión cumplen con las identidades del tipo

$$R \cap (S \cup T) = (R \cap S) \cup (R \cap T),$$
$$R \cup (S \cap T) = (R \cup S) \cap (R \cup T),$$

cuyas comprobaciones dejamos al lector en calidad de ejercicio. Los dibujos





ayudarán a realizar los razonamientos sencillos requeridos.

Se llama *diferencia* $S \setminus T$ de dos conjuntos S y T, al cúmulo de elementos de S, que no pertenecen a T. Aquí, en general, no se supone que $T \subset S$. En lugar de $S \setminus T$ se escribe también $S - T$.

Si T es un subconjunto en S, entonces el símbolo $S \setminus T$ indica además *suplemento* de T en S. Haciendo $R = S \setminus T$, tendremos: $R \cap T = \varnothing$, $R \cup T = S$ Prestemos atención a la correspondencia

entre las operaciones de intersección, unión, suplementación, y las uniones lógicas «y», «o», «no».

Sean X e Y dos conjuntos cualesquiera. El par de elementos (x, y), con $x \in X$, $y \in Y$, tomados en un orden dado, serán llamados *par ordenado*, considerando en este caso, que $(x_1, y_1) = (x_2, y_2)$ si y sólo si, $x_1 = x_2$, $y_1 = y_2$. Se llama *producto ortogonal* (o cartesiano) de dos conjuntos X e Y, al conjunto de todos los pares ordenados (x, y):

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}.$$

Sea, por ejemplo, el conjunto de todos los números reales $\mathbb{R}$. Entonces, *el cuadrado cartesiano* $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, es simplemente el conjunto de todas las coordenadas cartesianas de los puntos en el plano respecto a los ejes de coordenadas dados. En forma análoga se podía haber definido el producto cartesiano $X_1 \times X_2 \times X_3$ de tres conjuntos $(= (X_1 \times X_2) \times X_3 = X_1 \times (X_2 \times X_3))$, de cuatro, etc. Con $X_1 = X_2 = \ldots = X_k$ se escribe abreviadamente $X^k = X \times X \times X \times \ldots \times X$ y se dice que es un conjunto X a *la k-ésima potencia cartesiana*. Los elementos de X^k son las sucesiones, o filas $(x_1, x_2, \ldots, x_k)$ de longitud k.

Para sentir la diferencia entre los conjuntos $X \times Y$ y $X \cup Y$, tomemos en calidad de X e Y conjuntos de potencia finita (cardinales)

$$|X| = \text{Card } X = n, \quad |Y| = \text{Card } Y = m.$$

Entonces

$$|X \times Y| = nm, \quad \text{y} \quad |X \cup Y| = n + m - |X \cap Y|.$$

Si esto no es claro, entonces es necesario releer todas las definiciones.

2. Aplicaciones. El concepto de *aplicaciones* o *funciones*, juega un papel esencial en las matemáticas. Dados los conjuntos X e Y, la aplicación f con *dominio de definición* X y *codominio de existencia* Y, hace corresponder a cada elemento $x \in X$, el elemento $f(x) \in Y$, denotado también con los símbolos fx o f_x. Cuando $Y = X$ se habla también de *la transformación* f del conjunto X sobre sí mismo. Simbólicamente, la aplicación se escribe de forma $f: X \to Y$ o $X \xrightarrow{f} Y$. Se llama imagen de la aplicación f, al conjunto de todos los elementos de la forma $f(x)$:

$$\text{Im } f = \{f(x) \mid x \in X\} = f(X) \subset Y.$$

El conjunto

$$f^{-1}(y) = \{x \in X \mid f(x) = y\}$$

se llama *preimagen* del elemento $y \in Y$. Más generalmente, para $Y_0 \subset Y$, supongamos que

$$f^{-1}(Y_0) = \{x \in X \mid f(x) \in Y_0\} = \bigcup_{y \in Y_0} f^{-1}(y).$$

Si $y \in Y \setminus \text{Im } f$, entonces, evidentemente, $f^{-1}(y) = \varnothing$.

La aplicación $f\colon X \to Y$ se llama *exahustiva* o *sobreyectiva* (aplicación sobre), cuando $\operatorname{Im} f = Y$; ella se llama inyectiva, cuando de $x \neq x'$ sigue $f(x) \neq f(x')$. Finalmente, $f\colon X \to Y$ es *biyectiva* o *biunívoca*, cuando esta aplicación es al mismo tiempo sobreyectiva e inyectiva.

La igualdad $f = g$ de dos aplicaciones significa, por definición, que sus dominios correspondientes coinciden: $X \xrightarrow{f} Y$, $X \xrightarrow{g} Y$ además $f(x) = g(x)$, $\forall x \in X$. La confrontación del «argumento» x, o sea del elemento $x \in X$, con el significado $f(x) \in Y$ se adopta representarla por medio de una flecha limitada $x \mapsto f(x)$.

Sea, por ejemplo, f_n un número de Fibonacci (véase el § 4) de una magnitud n. La correspondencia $n \mapsto f_n$ determina la aplicación $\mathbb{N} \to \mathbb{N}$, que no es sobreyectiva, lo que resulta evidente, ni inyectiva, por cuanto $f_1 = f_2 = 1$. Si $\mathbb{R}_+$ es el conjunto de los números reales positivos, entonces las aplicaciones $f\colon \mathbb{R} \to \mathbb{R}$, $g\colon \mathbb{R} \to \mathbb{R}_+$, $h\colon \mathbb{R}_+ \to \mathbb{R}_+$, definidas por una misma regla $x \mapsto x^2$, son todas diferentes: f no es ni sobreyectiva ni inyectiva; g es sobreyectiva pero no inyectiva; y la aplicación h es biyectiva. De este modo, todo lo concerniente al dominio de definición y al codominio de valores (o de existencia), es una parte esencial en la determinación de la aplicación (función).

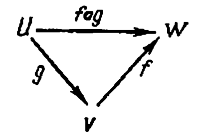
Se denomina aplicación *unidad* (o *idéntica*) $e_X\colon X \to X$ la que traslada cada elemento $x \in X$ sobre sí mismo. Si X es un subconjunto en Y: $X \subset Y$, entonces a veces resulta útil una aplicación especial, *la inclusión* $I\colon X \to Y$, que asocia a cada elemento $x \in X$ el mismo elemento, pero ya en el conjunto Y. La aplicación $f\colon X \to Y$ se llama *estrechamiento* (o *restricción* o *limitación*) de la aplicación $g\colon X' \to Y'$, cuando $X \subset X'$, $Y \subset Y'$ y $f(x) = g(x)$, $\forall x \in X$. A su vez g se llama *prolongación* de la aplicación f. Por ejemplo, la inclusión $I\colon X \to Y$ es limitación de la aplicación unidad $e_Y\colon Y \to Y$.

Tendremos oportunidad también de referirnos a funciones de muchas variables. Es útil aclararse a sí mismo, que el concepto arriba introducido de potencia cartesiana X^n del conjunto X permite hablar acerca de la función $f(x_1, \ldots, x_n)$ de múltiples variables $x_i \in X$, $i = 1, \ldots, n$, como si fuera una aplicación común $f\colon X^n \to Y$.

Producto (*superposición* o *composición*) de dos aplicaciones $g\colon U \to V$ y $f\colon V \to W$ se llama la aplicación $f \circ g\colon U \to W$, definida por las condiciones

$$(f \circ g)(u) = f(g(u)), \quad \forall u \in U.$$

Lo mismo, claramente, se muestra en *el diagrama triangular*



De este diagrama se dice, que «conmuta» (o *es conmutativo*), o sea, que el resultado del paso desde U hacia W no depende si lo damos directamente, con ayuda de $f \circ g$, o utilizamos la etapa intermedia V. Obsérvese que la composición no está definida para cualesquiera aplicaciones f y g. Es necesario que en las notaciones anteriores, el conjunto V fuese común a ambas. Pero la composición de dos transformaciones del conjunto X en sí mismo, siempre tiene sentido.

En adelante, en lugar de $f \circ g$ escribiremos sencillamente g.

Es claro que

$$fe_X = f, \quad e_Y f = f$$

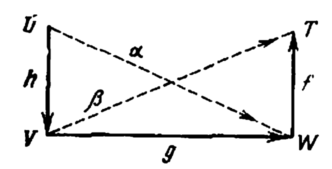
para cualquier aplicación $f\colon X \to Y$. La prueba de esta propiedad es evidente.

A una importante propiedad de la composición (producto) de una aplicación, se refiere el siguiente

TEOREMA 1. *La composición de aplicaciones obedece a la ley de asociatividad. Esto significa que, si* $h\colon U \to V$, $g\colon V \to W$, $f\colon W \to T$, son tres aplicaciones, entonces

$$f(gh) = (fg)\,h.$$

DEMOSTRACION. Visualmente, todos los razonamientos necesarios están contenidos en el diagrama siguiente:



donde $\alpha = gh$, $\beta = fg$. En correspondencia con la definición formal de igualdad de aplicaciones, sólo es necesario comparar los valores de las aplicaciones $f(gh)\colon U \to T$ y $(fg)\,h\colon U \to T$ en un «punto» cualquiera $u \in U$. Pero, de acuerdo con la definición de composición de aplicaciones, tenemos

$$(f(gh))\,u = f((gh)\,u) = f(g(hu)) = (fg)(hu) = ((fg)\,h)\,u. \blacksquare$$

La composición de las aplicaciones $X \to X$, en general, no es conmutativa, o sea $fg \neq gf$. Resulta fácil convencerse de esto en el ejemplo, cuando $X = \{a, b\}$ es un conjunto de dos elementos, $f(a) = b$, $f(b) = a$, $g(a) = a$, $g(b) = a$. Otro ejemplo: f y g son aplicaciones constantes de X en X, o sea, los valores de $f(x)$ y $g(x)$ no dependen de x. Entonces $f \neq g \Rightarrow fg \neq gf$.

Algunas funciones tienen *inversas*. Supongamos que $f\colon X \to Y$ y $g\colon Y \to X$ son dos aplicaciones tales, que las composiciones fg y gf están determinadas. Si $fg = e_Y$, entonces f se llama *inversa por*

la izquierda respecto a g, y g es *inversa por la derecha* respecto a f. Cuando el producto, en cualquier orden que se lo realice, da como resultado una aplicación idéntica:

$$fg = e_Y, \quad g_Yf = e_X, \tag{1}$$

entonces g se llama *aplicación inversa hacia ambos lados* (o simplemente *inversa*) para f, o con respecto a f (y f es aplicación inversa respecto a g), y se designa con el símbolo f^{-1}. Y bien, $f(u) = y \Leftrightarrow \Leftrightarrow f^{-1}(v) = u$.

Suponiendo también la existencia de otra aplicación $g'\colon Y \to X$ para la cual

$$fg' = e_Y, \quad g'f = e_X, \tag{1'}$$

basándonos en las igualdades de (1) y (1') y en el teorema 1, obtenemos

$$g' = e_Xg' = (gf)\,g' = g\,(fg') = ge_Y = g.$$

De este modo, la aplicación inversa para ambos lados respecto a f si es que existe, está determinada unívocamente. Esto sirve para convalidar la notación f^{-1}.

TEOREMA 2. *La aplicación $f\colon X \to Y$ tiene inversa si, y sólo si, es recíprocamente unívoca (biyectiva).*

LA DEMOSTRACION de este teorema se basa en el lema siguiente, que tiene un interés particular.

LEMA. *Si $f\colon X \to Y$, $g\colon Y \to X$ son dos aplicaciones cualesquiera, para las cuales $gf = e_X$, entonces f es inyectiva, y g es sobreyectiva.*

De hecho, sea $x, x' \in X$ y $f(x) = f(x')$. Entonces $x = e_X(x) = (gf)\,x = g\,(fx) = g\,(fx') = (gf)\,x' = e_X(x') = x'$. Por lo visto f es inyectiva. Si, de seguido, x es un elemento cualquiera de X, entonces $x = e_X(x) = (gf)\,x = g\,(fx)$, y esto demuestra la sobreyectividad de g.

Volviendo al teorema 2, supongamos, al principio, que f tiene inversa $g = f^{-1}$. Entonces, de las igualdades (1) y del lema se deduce tanto la sobreyectividad, como la inyectividad de f. En otras palabras, f es biyectiva. Por el contrario, suponiendo a f biyectiva, encontraremos para cualquier $y \in Y$ un **único** elemento $x \in X$, para el cual $f(x) = y$. Haciendo $g(y) = x$, definimos la aplicación $g\colon Y \to X$, que tiene las propiedades de (1). Significa, que $f^{-1} = g$. ∎

COROLARIO. *De la biyectividad de la aplicación $f\colon X \to Y$ se deduce la biyectividad de f^{-1}, además*

$$(f^{-1})^{-1} = f. \tag{2}$$

Sea, después, $f\colon X \to Y$, $h\colon Y \to Z$ un par de aplicaciones biyectivas. Entonces también será biyectiva su composición hf, además

$$(hf)^{-1} = f^{-1}h^{-1}. \tag{3}$$

DEMOSTRACIÓN. De acuerdo al teorema 2, la biyectividad de f trae aparejada la existencia de f^{-1}, que, en virtud del mismo teorema, equivale a la biyectividad de f^{-1}. La simetría de las condiciones de (1) reescritas de la forma $ff^{-1} = e_Y$, $f^{-1}f = e_X$, da la igualdad (2). Siguiendo, de acuerdo a las condiciones y al teorema 2, existen las aplicaciones $f^{-1}: Y \to X$, $h^{-1}: Z \to Y$ y su composición $f^{-1}h^{-1}: Z \to X$. De las igualdades

$$(hf)(f^{-1}h^{-1}) = ((hf)f^{-1})h^{-1} = (h(ff^{-1}))h^{-1} = hh^{-1} = e_Z,$$
$$(f^{-1}h^{-1})(hf) = f^{-1}(h^{-1}(hf)) = f^{-1}((h^{-1}h)f) = f^{-1}f = e_X$$

se deduce, que $g^{-1}h^{-1}$ es la aplicación inversa con respecto a hf. ∎

La aplicación «de seguimiento» $\sigma: \mathbb{N} \to \mathbb{N}$, definida por la regla $\sigma(n) = n + 1$, es inyectiva, pero no sobreyectiva, por cuanto el primer elemento (la unidad) no pertenece a la $\operatorname{Im} \sigma$. Es interesante el hecho de que, para los conjuntos finitos, una situación semejante es imposible.

TEOREMA 3. *Si X es un conjunto finito, y la transformación $f: X \to X$ es inyectiva, entonces ésta es biyectiva.*

DEMOSTRACION. Es sólo necesario mostrar, que f es sobre yectiva, o sea, que para cualquier elemento $x \in X$ se halla un x' con $f(x') = x$. Hagamos

$$f^k(x) = f(f \ldots (fx) \ldots) = f(f^{k-1}x), \quad k = 0, 1, 2, \ldots$$

En virtud que X es finito, en esta sucesión de elementos deberá haber repeticiones. Sea, digamos, $f^m(x) = f^n(x)$, $m > n$. Si $n > 0$ entonces, de $f(f^{m-1}x) = f(f^{n-1}x)$ y de la inyectividad de f, sigue la igualdad $f^{m-1}(x) = f^{n-1}(x)$. Repitiendo un número suficiente de veces la reducción de f, llegaremos al elemento $x' = f^{m-n-1}(x)$ con la propiedad requerida: $f(x') = x$. ∎

Como es fácil de comprender, *la transformación sobreyectiva de un conjunto finito en sí mismo, es también biyectiva.*

Algunas palabras sobre potencia. Se considera que dos conjuntos X e Y tienen igual potencia si, y sólo si, existe una aplicación biyectiva $f: X \to Y$. Los conjuntos de la misma potencia que $\mathbb{N}$ (o $\mathbb{Z}$), se llaman conjuntos numerables.

EJRECICIOS

1. Sea $\Omega = \{+, -, ++, +-, -+, --, +++, \ldots\}$ el conjunto de todas las sucesiones de «más» y «menos», y $f: \Omega \to \Omega$ una transformación, que traslada el elemento $\omega = \omega_1\omega_2 \ldots \omega_n \in \Omega$ a $\omega' = \omega_1\bar{\omega}_1\omega_2\bar{\omega}_2 \ldots \omega_n\bar{\omega}_n$, donde $\bar{\omega}_k = -$, si $\omega_k = +$, y $\bar{\omega}_k = +$, si $\omega_k = -$. Mostrar que en $f(f\omega)$ cualquier segmento de longitud > 4 contiene $++0--$.

2. ¿Tendrá la aplicación $f: \mathbb{N} \to \mathbb{N}$, dada de acuerdo a la regla $n \mapsto n^2$, inversa por la derecha? Indicar para f dos aplicaciones inversas por la izquierda.

3. Sean $f: X \to Y$ una aplicación y S, T dos subconjuntos en X. Mostrar

que

$$f(S \cup T) = f(S) \cup f(T), \quad f(S \cap T) \supset f(S) \cap f(T).$$

Dar un ejemplo que muestre que la última inclusión no se puede, en general, sustituir por una igualdad.

4. El símbolo $\mathcal{P}(S) = \{T \mid T \subset S\}$ designa al conjunto de todos los subconjuntos de S. Si, por ejemplo, $S = \{s_1, s_2, \ldots s_n\}$ es un conjunto finito de n elementos, entonces $\mathcal{P}(S)$ está compuesto por el conjunto vacío $\varnothing$, por n conjuntos de un elemento $\{s_1\}, \{s_2\}, \ldots, \{s_n\}$, por $n(n-1)/2$ conjuntos $\{s_i, s_j \mid 1 \leqslant i < j \leqslant n\}$ y así sucesivamente, hasta $T = S$. ¿Cuál es la potencia del conjunto $\mathcal{P}(S)$?

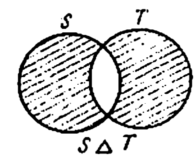
5. Sea una aplicación $f\colon X \to Y$, y $b = f(a)$ para cierto $a \in X$. A la preimagen

$$f^{-1}(b) = f^{-1}(f(a)) = \{x \mid f(x) = f(a)\}$$

a veces la llaman también *estrato* sobre el elemento $b \in \operatorname{Im} f$. Demostrar, que todo el conjunto X es resultado de la unión de estratos no intersecados (partición del conjunto X). Advertencia: el símbolo $f^{-1}(b)$ no se debe asociar con la aplicación inversa, que puede no existir.

6. Mostrar que la potencia (grado) cartesiana de un conjunto par, es un conjunto numerable.

7. El símbolo $S \triangle T$ significa la diferencia simétrica de dos conjuntos S y T:



$$S \triangle T = (S \setminus T) \cup (T \setminus S).$$

Mostrar que

$$S \triangle T = (S \cup T) \setminus (S \cap T).$$

§ 6. RELACIONES DE EQUIVALENCIA. FACTORIZACIONES DE LAS APLICACIONES

La equivalencia de sistemas de ecuaciones lineales fue formulada en el § 3, y sugiere considerar este concepto en un plano general, sobre todo siendo que las equivalencias de distintos tipos se usan con significados diversos, tanto en los razonamientos lógicos, como en la vida diaria.

1. Relaciones binarias. Para dos conjuntos cualesquiera X e Y cualquier subconjunto $O \subset X \times Y$ se denomina *relación binaria* entre X e Y (o sencillamente en X, si $Y = X$). Para el par ordenado $(x, y) \in O$ se usa el símbolo xOy y se dice, que x se encuentra en relación O respecto a y. Esto es cómodo, por cuanto, por ejemplo, el ordenamiento «$<$» en el conjunto de los números reales $\mathbb{R}$ es una relación binaria en $\mathbb{R}$, compuesta de todos los puntos del plano $\mathbb{R}^2$, que se encuentran por encima de la recta $x - y = 0$ (véase la fig. 6); La voluminosa inclusión

$$(x, y) \in O \ (O = <)$$

es sustituida por la habitual desigualdad $x < y$.

A cada función $f\colon X \to Y$ se le confronta su *gráfica*, el subconjunto

$$\Gamma(f) = \{(x, y) \mid x \in X, \quad y = f(x)\} \subset X \times Y,$$

que indica la relación entre X e Y. El estudio de las gráficas de las funciones $\mathbb{R} \to \mathbb{R}$ en $\mathbb{R}^2$, es parte del curso de análisis matemático. Se comprende, que no cada relación O puede servir de gráfica de

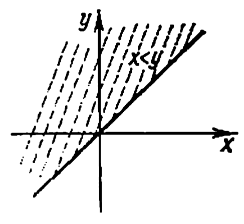


Fig.6

alguna aplicación $X \to Y$. La condición necesaria y suficiente se reduce a que, a cada $x \in X$ responda exactamente un elemento y con xOy. Las X e Y dadas, así como las gráficas $\Gamma(f)$ reconstituyen a f.

2. **Relación de equivalencia.** La relación binaria $\sim$ en X se llama *relación de equivalencia*, si para toda $x, x', x'' \in X$ se cumplen las condiciones:

(i) $x \sim x$ (*reflexividad*);

(ii) $x \sim x' \Rightarrow x' \sim x$ (*simetría*);

(iii) $x \sim x', x' \sim x'' \Rightarrow x \sim x''$ (*transitividad*).

La escritura $a \nsim b$ expresa la negación de la equivalencia entre los elementos $a, b \in X$.

El subconjunto

$$\bar{x} = \{x' \in X \mid x' \sim x\} \subset X$$

de todos los elementos equivalentes a un x dado, se denomina *clase de equivalencia* contenedora de x.

Como $x \sim x$ (ver (i)), entonces, efectivamente $x \in \bar{x}$. Cualquier elemento $x' \in \bar{x}$ se llama representante de la clase $\bar{x}$.

Es justa la afirmación siguiente.

El conjunto de clases de equivalencia en la relación $\sim$ es partición del conjunto X en el sentido que X es la unión de subconjuntos disjuntos (esta partición se puede designar con el símbolo $\sim \pi(X)$).

De hecho, como $x \in \bar{x}$, entonces $X = \bigcup_{x \in X} \bar{x}$. Seguidamente, la clase $\bar{x}$ se determina unívocamente por medio de cualquiera de sus representantes, o sea, $\bar{x} = \bar{x}' \Leftrightarrow x \sim x'$. De un lado $x \sim x'$

y $x'' \in \bar{x} \Rightarrow x'' \sim x \Rightarrow x'' \sim x' \Rightarrow x'' \in \bar{x}' \Rightarrow \bar{x} \subset \bar{x}'$. Pero $x \sim x' \Rightarrow x' \sim \sim x$ (véase (ii)). Por eso, también se cumple la inclusión inversa $\bar{x}' \subset \bar{x}$. O sea, $\bar{x}' = \bar{x}$. Por otro lado: tal como $x \in \bar{x}$ entonces $\bar{x}' = \bar{x} \Rightarrow x \in \bar{x}' \Rightarrow x \sim x'$.

Si ahora $\bar{x}' \cap \bar{x}'' \neq \varnothing$ y $x \in \bar{x}' \cap \bar{x}''$, entonces $x \sim x'$ y $x \sim x''$, de donde, debido a la transitividad (iii) tenemos $x' \sim x''$ y $\bar{x}' \sim \bar{x}''$. O sea, las distintas clases no se intersecan. ∎

Sea $\Pi = R^2$ un plano real con un sistema de coordenadas rectangulares (cartesianas).

Tomando como propiedad de $\sim$ la pertenencia de los puntos P, $P' \in \Pi$ a una recta horizontal, obtenemos, evidentemente, una relación de equivalencia

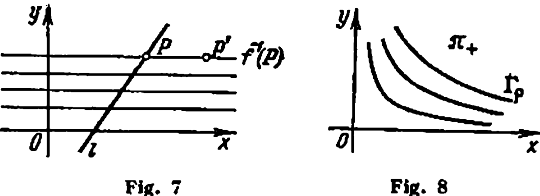


Fig. 7 Fig. 8

con clases de rectas horizontales (fig. 7). Las hipérbolas $\Gamma\rho$ (fig. 8) del tipo $xy = \rho > 0$, determinan la relación de equivalencia en el campo $\Pi_+ \subset \Pi$ de los puntos $P(x, y)$ con coordenadas $x > 0$, $y > 0$. Estos ejemplos geométricos, muestran en forma clara, que es cierta la siguiente afirmación.

Si se tiene alguna partición $\pi(X)$ del conjunto X en subconjuntos disjuntos C_x, entonces, los C_x serán clases de equivalencia por alguna relación de equivalencia $\sim$.

De hecho, según la condición cada elemento $x \in X$ está exactamente contenido en un subcojunto C_a. Es suficiente considerar $x \sim x'$ si, y sólo si, x y x' pertenecen a un mismo subconjunto C_a. Evidentemente, la relación $\sim$ es reflexiva, simétrica y transitiva, o sea, es relación de equivalencia. Seguidamente, $x \in C_a \Rightarrow \bar{x} = C_a$, por cuanto por definición de $\sim$ tenemos la inclusión $\bar{x} \subset C_a$, y $C_a \subset \subset \bar{x}$ se deduce de que distintos C_t no se intersecan de dos en dos. Por lo visto, $\pi(X) = \pi_\sim(X)$. ∎

3. Factorización de las aplicaciones. En vista de la correspondencia mutuamente unívoca, establecida arriba, entre las relaciones de equivalencia y las particiones del conjunto X; es usual designar con el símbolo $X/\sim$, y llamar *conjunto cociente S* respecto a $\sim$ (o en relación a $\sim$), a la partición que cumple la relación de equivalencia $\sim$. La aplicación sobreyectiva

$$p : x \mapsto p(x) = \bar{x} \quad (1)$$

se llama *aplicación natural* (o *proyección canónica*) de X en el conjunto cociente $X/\sim$.

Sean X e Y dos conjuntos y $f\colon X \to Y$ una aplicación. La relación binaria O_f:

$$xO_fx' \Leftrightarrow f(x),\ f(x')\ \forall x,\ x' \in X,$$

evidentemente, es reflexiva ($f(x) = f(x)$), simétrica ($f(x') = f(x) \Rightarrow f(x) = f(x')$) y transitiva ($f(x) = f(x')$ y $f(x') = f(x'') \Rightarrow f(x) = f(x'')$). De este modo, O_f es una relación de equivalencia en X. Las clases correspondientes de equivalencia $\bar{x}$ son estratos (preimágenes) en el sentido del ejercicio 5 del § 5. En otras palabras,

$$\bar{x} = \{x' \mid f(x') = f(x)\}.$$

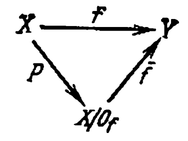
La aplicación $f\colon X \to Y$ *induce* la aplicación $\bar{f}\colon X/O_f \to Y$, definida por la regla

$$\bar{f}(\bar{x}) = f(x), \tag{2}$$

o, lo que es lo mismo,

$$\bar{f}p(x) = f(x), \tag{2'}$$

donde p es la aplicación natural (1). Como $\bar{x} = \bar{x}' \Leftrightarrow f(x) = f(x')$, entonces la relación (2), que prefija $\bar{f}$, no depende de la elección del representante x de la clase $\bar{x}$. En tales casos se dice que la definición $\bar{f}$



es *cierta* o *correcta*. El diagrama conmutativo describe claramente la *factorización* (*descomposición*)

$$f = \bar{f} \cdot p \tag{3}$$

de la aplicación f en el producto de la aplicación sobreyectiva p por la aplicación inyectiva $\bar{f}$. La inyectividad de $\bar{f}$ se deduce de que,

$$\bar{f}(\bar{x}_1) = \bar{f}(\bar{x}_2) \Leftrightarrow f(x_1) = f(x_2) \Leftrightarrow \bar{x}_1 = \bar{x}_2.$$

La biyectividad de f equivale a la sobreyectividad de $\bar{f}$. Observemos, que si $f'\colon X/O_f \to Y$ es otra aplicación, para la cual se cumple la relación (3): $f'p = f$, entonces, de $f'(\bar{x}) = f'(px) = (f'p)x = f(x) = \bar{f}(\bar{x})$ (véase (2)), sigue de hecho la igualdad $f' = \bar{f}$. Por lo visto, la aplicación $\bar{f}$, que hace conmutativo al diagrama triangular indicado arriba, es única.

4. Conjuntos ordenados. Se llama ordenación del conjunto X (u *orden en* X), la relación binaria $\leqslant$ en X, que tiene las propiedades de reflexión ($x \leqslant x$), antisimetría (si $x \leqslant y$ e $y \leqslant x$, entonces $x = y$) y transitividad (si $x \leqslant y$ e $y \leqslant z$, entonces $x \leqslant z$). Cuando $x \leqslant y$ y $x \neq y$ se escribe $x < y$. En lugar de $x \leqslant y$ se usa también la notación $y \geqslant x$. El par de elementos x, $x' \in X$ puede no encontrarse en relación $\leqslant$. Sin embargo, si $x \leqslant x'$ o $x' \leqslant x$ para cada

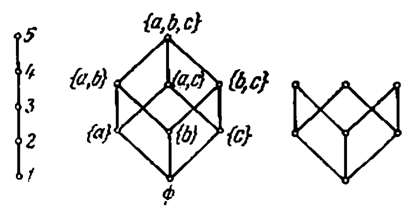


Fig. 9

par de elementos de X, entonces X se denomina conjunto *linealmente ordenado* (o conjunto *completamente ordenado*, *cadena*, etc.). En un caso general se hace referencia a un *orden parcial* en X.

El conjunto $X = \mathscr{P}(S)$ de los subconjuntos del conjunto S (véase el ejercicio 4 del § 5) con relaciones comunes de inclusión $R \subset T$ entre los subconjuntos, y también el conjunto $\mathbb{N}$ de números naturales con la relación $d \mid n$ (n se divide por d), son ejemplos de conjuntos parcialmente ordenados.

Sea X un conjunto parcialmente ordenado cualquiera, x e y sus elementos. Se dice, que *y cubre* a x, si $x < y$ y no existe ningún z tal que $x < z < y$. En caso que Card $X < \infty$, $x < y$ si, y sólo si, se halla una sucesión de elementos $x = x_1, x_2, \ldots, x_{n-1}, x_n = y$, en la cual x_{i+1} cubre a x_i (en otras palabras: esta es también la condición necesaria para que x e y sean comparables). El concepto de cobertura es cómodo para la representación de un conjunto finito parcialmente ordenado X, por un diagrama plano. Los elementos del conjunto X se representan con puntos. Si y cubre a x, entonces y se coloca por encima de x, y x se une con y por medio de un segmento de recta. La comparabilidad entre y y x se indica por una línea quebrada «en descenso», que une a y con x, pudiendo haber varias líneas quebradas. Las x e y no comparables no se unen. En dos de los diagramas presentados (véase la fig. 9) se han trazado «segmentos» de la serie natural de números y el conjunto $\mathscr{P}(\{a, b, c\})$ ($\mathbb{N}$ es un conjunto natural linealmente ordenado, y el ordenamiento en $\mathscr{P}(S)$ fue introducido antes).

Se llama *elemento mayor n*, de un conjunto parcialmente ordenado X a $n \in X$ tal que $x \leqslant n$ para todo $x \in X$; y elemento máximo

$m \in X$, al que, cumpliendo con $m \leqslant x \in X$, hace $x = m$. El elemento mayor es siempre máximo, pero no viceversa. Puede haber muchos elementos máximos, pero el elemento mayor, si existe, está determinado unívocamente. Las mismas observaciones se refieren a *los elementos menor y mínimo*. En la fig. 9, los dos diagramas de la izquierda tienen elementos mayor y menor. En el diagrama de la derecha hay tres elementos máximos, un menor, pero no existe elemento mayor.

La teoría de los sistemas algebraicos parcialmente ordenados (álgebra de Boole, retículos), saturada de resultados sustanciales, ocupa un lugar importante en el álgebra, pero no tenemos posibilidades de referirnos a ella. Este parágrafo persigue un fin modesto: presentar al lector otra relación binaria natural, y darle una idea acerca de los diagramas, que ayudarán en el futuro a comprender la posición mutua de los subgrupos en los grupos o, digamos, la disposición de los subcampos en los campos.

EJERCICIOS

1. Mostrar, que el conjunto cociente $\mathbb{R}^2/\sim$ que se obtiene del dibujo geométrico de la fig. 7, y cualquier recta l, que corta al eje Ox, se encuentran en correspondencia biyectiva.

2. Hacer $P(x, y) \sim P(x', y')$ para los puntos de coordenadas reales del plano $\mathbb{R}^2$ exactamente, cuando $x' - x \in \mathbb{Z}$ o $y' - y \in \mathbb{Z}$.

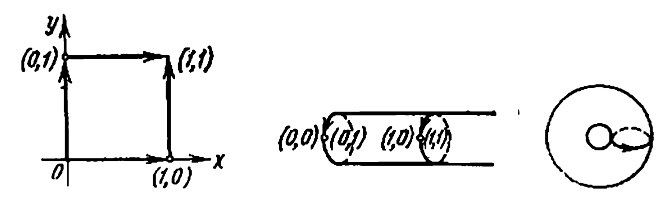


Fig. 10

Demostrar, que $\sim$ es relación de equivalencia y que el conjunto cociente $\mathbb{R}^2/\sim$ geométricamente se ilustra por los puntos en el torso (superficies de «contorno»; véase la fig. 10).

3. Mostrar que los conjuntos de dos, tres y cuatro elementos, tienen, respectivamente, 2, 5 y 15 conjuntos cocientes distintos.

4. Sea $\sim$ una relación de equivalencia en el conjunto X, y $f\colon X \to Y$ una aplicación para la que $x \sim x' \Rightarrow f(x) = f(x')$. Mostrar que esta condición de *compatibilidad* de f con $\sim$ (más débil que la considerada en el punto 2) permite determinar correctamente la aplicación inducida $\bar{f}\colon \bar{x} \mapsto f(x)$, de $X/\sim$ en Y, que lleva a la factorización $f = \bar{f} \cdot \bar{\bar{p}}$, pero $\bar{f}$ ya no será necesariamente inyectiva. ¿A qué se reduce la condición de inyectividad de $\bar{f}$?

5. Trazar los diagramas de los conjuntos parcialmente ordenados: 1) $\mathcal{P}(\{a, b, c, d\})$; 2) conjunto de todos los divisores del número entero 24 (las relaciones de ordenamiento están indicadas en el texto).

§ 7. PRINCIPIO DE INDUCCIÓN MATEMÁTICA

Se considera que nos es conocido el conjunto $\mathbb{N} = \{1, 2, 3, \ldots\}$ de todos los números *naturales* (*enteros positivos*). De hecho, como punto de partida para el estudio de $\mathbb{N}$ sirve la axiomática de Peano (1858—1932). De sus tres axiomas (que no exponemos) surgen las propiedades de suma, multiplicación y ordenamiento lineal (véase el punto 4 del § 6) de los números naturales o, más exactamente, del sistema $\mathbb{N} \cup \{0\}$. En particular, se demuestra esta afirmación que es intuitivamente clara: *en cada conjunto no vacío* $S \subset \mathbb{N}$ *hay un elemento menor*, o sea, un número natural $s \in S$ más pequeño que los demás números en S. Teniendo en cuenta esta afirmación de los axiomas de Peano se extrae el siguiente

PRINCIPIO DE INDUCCIÓN. *Supongamos, que para cada $n \in \mathbb{N}$ tenemos alguna afirmación $M(n)$. Supongamos también que disponemos de una regla que nos permite establecer la veracidad de $M(l)$ para un l dado, con la condición de que $M(k)$ es cierto para todo $k < l$ (en particular se sobreentiende que podemos verificar la veracidad de M (1). Entonces, $M(n)$ es cierto para todo $n \in \mathbb{N}$.*

De hecho, admitamos que el subconjunto

$$S = \{s \mid s \in \mathbb{N},\ M(s) \text{ inexacto}\} \subset \mathbb{N}$$

no es vacío. De acuerdo a lo antedicho, S contiene al elemento menor s_0. Entonces, la afirmación $M(s_0)$ es falsa, y $M(s)$ es verdadera para cada $s < s_0$. Esto, sin embargo, contradice nuestra supuesta capacidad para demostrar la veracidad de $M(s_0)$. ∎

No es éste el lugar para una discusión profunda del principio de inducción matemática. Nos limitaremos a observar que él refleja, por así decir, la esencia de la serie natural, y el conocimiento de esta última no conduce a algo que sea fundamentalmente más sencillo.

Cabe prestar atención a otra circunstancia más. Precisamente, un momento indispensable en la «demostración por el método de inducción completa», resulta el establecimiento de la *base de la inducción*, o sea, la comprobación de que la propiedad o la afirmación es cumplida para n pequeños. Sin esta comprobación se puede llegar a conclusiones arbitrarias del tipo «todos los estudiantes son de igual estatura». Veamos el razonamiento. El conjunto vacío de estudiantes y el conjunto de un estudiante aparte tienen esta propiedad. Formulamos el presupuesto de inducción, que esta propiedad la tiene cualquier conjunto de $\leqslant n$ estudiantes. En el conjunto de $n + 1$ estudiantes, los primeros n y los últimos n son de igual estatura por presupuesto de inducción. Estos conjuntos se intersecan con el subconjunto de $n - 1$ estudiantes, también de igual estatura. Esto significa que todos los $n + 1$ estudiantes son de igual estatura. De hecho, la primera afirmación de contenido se refería a un con-

junto de cualesquiera dos estudiantes, pero aquí precisamente resulta esto falso. ¿Qué longitud debe tener la fundamentación (la base) de la inducción? Frecuentemente esto queda claro de la demostración. En nuestro ejemplo elemental, lo importante es la condición de que la intersección de dos conjuntos no resulte un conjunto vacío, o sea, el cumplimiento de la desigualdad $n - 1 \geqslant 1$, de donde $n \geqslant 2$.

En situaciones más complejas, en especial cuando hay que definir o construir un objeto por inducción, con ayuda de relaciones de recurrençia (como nos proponemos construir determinantes de las matrices, en el capítulo 3), hay que prestar especial atención a la base de la inducción. Por otra parte, no se puede caer en el otro extremo: convencidos de la veracidad de $M(k)$ para todos los k de un segmento suficientemente largo $1 \leqslant k \leqslant l$ de la serie natural, concluír sin fundamento la veracidad de $M(n)$ para todo $n \in \mathbb{N}$ (lo que es, la denominada inducción incompleta).

He aquí dos ejemplos desalentadores.

1. P. Fermat suponía que todos los números del tipo $F_n = 2^{2^n} + 1$, $n = 0, 1, \ldots$ (*números de Fermat*) eran primos. Los primeros cinco números de Fermat son primos, pero para F_5 Euler halló la descomposición $F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$. Los esfuerzos actuales para obtener, con ayuda de las novísimas computadoras, aunque sea sólo un nuevo número de Fermat, hasta ahora no han tenido éxito. Uno de los últimos «progresos» en este sentido, ha sido la comprobación de que F_{1945} se divide por $5 \cdot 2^{1947} + 1$.

2. La investigación de los números del tipo $n^2 - n + 41$ cuando $n = 1, 2, \ldots, 40$ (o sea, del polinomio propuesto por Euler), es capaz de hacernos pensar que estos números son primos para cualquier n (acerca de los números primos véase § 8). Sin embargo, $41^2 - 41 + 41 = 41^2$.

Ejemplos de este género, pueden brindarse en cantidad.

En los razonamientos por inducción, a veces lo más importante es darle la forma debida a la afirmación que se demuestra. Supongamos que hay que hallar la suma

$$p_k(n) = 1^k + 2^k + 3^k + \ldots + (n-1)^k + n^k; \quad k = 1, 2, 3.$$

El problema se facilita considerablemente, cuando a Ud. le dicen que la presunta respuesta está contenida en las expresiones:

$$p_1(n) = \frac{n(n+1)}{2}, \quad p_2(n) = \frac{n(n+1)(2n+1)}{6} \quad p_3(n) = \left[\frac{n(n+1)}{2}\right]^2.$$

Si bien a $p_1(n)$ no es difícil llegar a pensarlo (lo que hizo Gauss a temprana edad), las formas $p_2(n)$ y $p_3(n)$ ya no son tan triviales, y la relación

$$p_5(n) + p_7(n) = 2\left[\frac{n(n+1)}{2}\right]^4$$

en general habría que haberla buscado por algún plan determinado. En el caso dado, se puede indicar este plan, pero no es ésta la cuestión.

Para la fundamentación de todas las relaciones indicadas arriba, es necesario realizar el paso de inducción de n a $n+1$ por cálculos directos. Dejamos esto al lector, en calidad de ejercicio útil.

A propósito, en éste ejercicio sirve la denominada *fórmula binomial*

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \ldots + \binom{n}{k} a^{n-k}b^k + \ldots + b^n. \quad (1)$$

Aquí a y b son números arbitrarios, y *el coeficiente binomial* $\binom{n}{k}$ del término $e^{n-k}b^k$ tiene la forma

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n\,(n-1)\,\ldots\,(n-k+1)}{k\,(k-1)\,\ldots\,2\cdot 1}. \quad (2)$$

Es útil completar (2) con la convención de que $0! = 1$ y de que $\binom{n}{k} = 0$ cuando $k < 0$. Observemos también que,

$$\binom{n}{n-k} = \binom{n}{k}$$

(propiedad de simetría de los coeficientes binomiales).

La fórmula (1) es cierta para $n = 1$, 2, evidentemente, y nosotros demostraremos por inducción que es cierta para n. Contando con su legitimidad para todos los índices $\leqslant n$, multiplicamos ambas partes de la relación (1) por $a+b$. Obtenemos

$$\begin{aligned}(a+b)^{n+1} &= (a+b)^n (a+b) = \\ &= a^n (a+b) + \ldots + \binom{n}{k} a^{n-k}b^k (a+b) + \ldots + b^n (a+b) = \\ &= a^{n+1} + a^n b + \ldots + \binom{n}{k-1} a^{n+2-k}b^{k-1} + \binom{n}{k-1} a^{n+1-k}b^k + \\ &\qquad + \binom{n}{k} a^{n+1-k}b^k + \binom{n}{k} a^{n-k}b^{k+1} + \ldots + ab^n + b^{n+1}.\end{aligned}$$

La reducción de los miembros semejantes muestra que, el coeficiente del término $a^{n+1-k}b^k$ será

$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!\,(n-k+1)!} + \frac{n!}{k!\,(n-k)!} = \\ &= \frac{n!}{(k-1)!\,(n-k)!}\left[\frac{1}{n-k+1} + \frac{1}{k}\right] = \\ &= \frac{n!}{(k-1)!\,(n-k)!} \cdot \frac{n+1}{k\,(n-k+1)} = \frac{(n+1)!}{k!\,(n+1-k)!} = \binom{n+1}{k},\end{aligned}$$

o sea, un coeficiente binomial del tipo (2) con el índico superior aumentado en una unidad. Por eso mismo, la veracidad de la fórmula (1) queda demostrada para todo $n \in \mathbf{N}$.

Si se escribe

$$(a+b)^n = (a+b)\,(a+b)\,\ldots\,(a+b),$$

adjudicando a cada factor del segundo miembro, números de 1 a n, y examinar aquellos subconjuntos de números $1 \leqslant i_1 < i_2 < \ldots$ $\ldots < i_k \leqslant n$, que al ser multiplicados responden al término $a^{n-k}b^k$, entonces llegaremos a la conclusión, que $\binom{n}{k}$ *no es otra cosa que el número de todos los subconjuntos de potencia* k, *de un conjunto de* n *elementos*. El número, un poco pasado de moda, $C_n^k = \binom{n}{k}$ de combinaciones de n sobre k, en esencia expresa lo mismo.

En particular, la potencia del conjunto $\mathcal{P}(\{s_1, \ldots, s_n\})$ (véase el ejercicio 4 del § 5) es igual a $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n-1} + \binom{n}{n}$. Pero, suponiendo que $a = b = 1$ en la fórmula (1), obtenemos

$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n}.$$

De este modo, Card $\mathcal{P}(\{s_1, s_2, \ldots, s_n\}) = 2^n$.

La demostración de un teorema o la construcción de un objeto, a veces es cómodo hacerlas apoyándose en formas más complejas de inducción. Por ejemplo, el principio de «inducción doble» consiste en lo siguiente: sea que dos números naturales cualesquiera m y n responden a alguna afirmación $Y(m, n)$, y al mismo tiempo: (i) $Y(m, 1)$ y $Y(1, n)$ se cumplen para todos los m y n; (ii) si $Y(k-1, l)$ e $Y(k, l-1)$ son ciertas, entonces $Y(k, l)$ también es cierta (equivalentemente: (ii)′ si $Y(k', l')$ es cierta para todos los $k' \leqslant k$, $l' \leqslant l$, $k' + l' < k + 1$, entonces $Y(k, l)$ es también cierta). Entonces, la afirmación $Y(m, n)$ es cierta para todos los números naturales m y n.

§ 8. ARITMÉTICA DE NÚMEROS ENTEROS

Es tarea de este parágrafo la suscinta descripción de las propiedades más sencillas de divisibilidad de los números enteros, a las que, por distintos motivos, resultará cómodo hacer referencia más adelante. En el capítulo 5 se expondrán hechos complementarios, debido a que la teoría de la divisibilidad se lleva a un sistema algebraico más general.

1. Teorema fundamental de la aritmética. El número entero s se llama *divisor* (o *multiplicador*) del número entero n, si $n = st$ para algún $t \in \mathbb{Z}$. A su vez, n se llama *múltiplo* de s. La divisibilidad de n por s se indica con el símbolo $s \mid n$, y a la indivisibilidad con el símbolo $s \nmid n$. La divisibilidad es una relación transitiva en $\mathbb{Z}$. Si, sucesivamente $m \mid n$ y $n \mid m$, entonces $n = \pm m$, y los números enteros m y n se llaman *asociados*. El número entero p, cuyos únicos divisores son los números $\pm p$, ± 1 (*divisores incompatibles*), se llama *primo*. Habitualmente, en calidad de primos, se toman los números primos positivos >1.

El rol fundamental de los números primos es puesto en claro por el denominado

TEOREMA FUNDAMENTAL DE LA ARITMETICA. *Cada número entero positivo $n \neq 1$ puede ser escrito en forma de un producto de números primos: $n = p_1 p_2 \ldots p_s$. Esta escritura es única con exactitud hasta el orden de los multiplicadores.*

Uniendo multiplicadores primos iguales y modificando sus notaciones, obtenemos una expresión de n de forma $n = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \ldots p_k^{\varepsilon_k}$, $\varepsilon_i > 0$, $1 \leqslant i \leqslant k$. Para cualquier número racional $a = n/m \in \mathbb{Q}$ tiene lugar una descomposición análoga, pero con exponentes ε_i tanto positivos como negativos. Observemos, que *el conjunto*

$$P = \{2, 3, 5, 7, 11, 13, \ldots\}$$

de todos los números primos, es infinito (teorema de Euclides). Por cierto, si sólo existiera una cantidad finita de números primos, digamos $p_1, p_2, \ldots, p_t$, entonces, de acuerdo al teorema fundamental, el número $c = p_1 p_2 \ldots p_t + 1$ sería divisible, por lo menos, por uno de los p_i. Sin limitación de comunidad consideramos a $c = p_1 c'$. Entonces, $p(c' - p_2 \ldots p_t) = 1$, y esto es imposible, por cuanto en $\mathbb{Z}$ divisores de la unidad son solamente ± 1. ∎

La demostración del teorema fundamental se pospone hasta el cap. 5. A primera vista, en general no hace falta demostrarlo, por lo evidente que parece. Entretanto, aun cuando se trata de las propiedades multiplicativas (propiedades divisivas) de los números enteros, no se puede demostrar el teorema principal sin efectuar a un mismo tiempo operaciones de multiplicación y de suma en $\mathbb{Z}$. En calidad ilustrativa de esta afirmación, examinemos en $\mathbb{N}$ al subconjunto $S = \{4k + 1 \mid k = 0, 1, 2, \ldots\}$. El es cerrado respecto al producto: $(4k_1 + 1) \times (4k_2 + 1) = 4k_3 + 1$. Por inducción, sobre $n \in S$, no es difícil establecer la existencia de una descomposición (primera parte del teorema fundamental) $n = q_1 \ldots q_l$, donde q_i son elementos de S que ya no pueden ser descompuestos. Los denominamos números cuasiprimos. Escribamos algunos de estos números: 5, 9, 13, 17, 21, 49. La segunda parte del teorema fundamental para el sistema S no es cierta, por cuanto, por ejemplo, el número $441 \in S$ tiene dos descomposiciones esencialmente distintas en productos de números cuasiprimos:

$$441 = 9 \cdot 49 = 21^2.$$

2. M.c.d. y m.c.m. en $\mathbb{Z}$. Dos números enteros cualesquiera n y m, pueden escribirse en forma de producto de los mismos números primos

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \quad m = \pm p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k},$$

si se acuerda en admitir a los exponentes nulos (como siempre considerando a $p_i^0 = 1$). Pongamos en consideración dos números enteros

$$\text{m.c.d.}\ (n, m) = p_1^{\nu_1} p_2^{\nu_2} \ldots p_k^{\nu_k}, \quad \text{m.c.m.}\ (n, m) = p_1^{\delta_1} p_2^{\delta_2} \ldots p_k^{\delta_k}, \tag{1}$$

donde $\nu_i = \min(\alpha_i, \beta_i)$, $\delta_i = \max(\alpha_i, \beta_i)$, $i = 1, 2, \ldots, k$. Como $d \mid n \Rightarrow d = \pm p_1^{\alpha_1'} \ldots p_k^{\alpha_k'}$, $0 \leqslant \alpha_i' \leqslant \alpha_i$, entonces, de las relaciones determinantes (1) se deducen las siguientes afirmaciones:

(i) m.c.d. $(n, m) \mid n$, m.c.d. $(n, m) \mid m$, y si $d \mid n$, $d \mid m$, entonces $d \mid$ m.c.d. (n, m).

(ii) $n \mid$ m.c.m. (n, m), $m \mid$ m.c.m. (n, m), y si $n \mid u$, $m \mid u$, entonces m.c.m. $(n, m) \mid u$.

Las propiedades (*i*) y (*ii*) justifican la simbolización reducida del máximo común divisor (m.c.d.) y del mínimo común múltiplo (m.c.m.) de los números enteros n, m. Para $n > 0$, $m > 0$ se cumple la relación

$$\text{m.c.d.}\ (n, m) \cdot \text{m.c.d.}\ (n, m) = nm. \qquad (2)$$

Los números enteros n, m se llaman *primos entre sí*, cuando m.c.d. $(n, m) = 1$. En este caso, la relación (2) toma la forma m.c.d. $(n, m) = nm$.

3. Algoritmo de división en $\mathbb{Z}$. Dados $a, b \in \mathbb{Z}$, $b > 0$, siempre *se hallarán* $q, r \in \mathbb{Z}$ tales que,

$$a = bq + r, \quad 0 \leqslant r < b$$

(*si considerar sólo los* $b \neq 0$, *entonces se cumplirá la desigualdad* $0 \leqslant r < |b|$).

Efectivamente, el conjunto $S = \{a - bs \mid s \in \mathbb{Z},\ a - bs \geqslant 0\}$, es, evidentemente, no vacío (por ejemplo, $a - b(-a^2) > 0$). Así que S contiene un elemento menor; designémoslo $r = a - bq$. Por condición $r \geqslant 0$. Suponiendo que $r \geqslant b$, obtendríamos el elemento $r - b = a - b(q + 1) \in S$, menor que r. Esta contradicción sólo se resuelve cuando $r < b$. ∎

Este sencillo razonamiento, llevado a cabo, da también la prescripción (*el algoritmo*) para hallar *al cociente b* y *al resto r* en un número finito de pasos. El algoritmo de división en $\mathbb{Z}$ se emplea para otra definición del m.c.d., y, en consecuencia, del m.c.m., si se toma en consideración la relación (2).

Precisamente, dados los números enteros n, m, conjuntamente no nulos, admitamos que

$$J = \{nu + mv \mid u,\ v \in \mathbb{Z}\}. \qquad (3)$$

Elegimos en J el menor elemento positivo $d = nu_0 + mv_0$. Utilizando el algoritmo de división, escribimos $n = dq + r$, $0 \leqslant r < d$. Habiendo elegido d, la inclusión

$$r = n - dq = n - (nu_0 + mv_0)\, q = n(1 - u_0 q) + m(-v_0 q) \in J$$

lleva a la igualdad $r = 0$. Así que $d \mid n$. Análogamente, se demuestra que $d \mid m$. Sea ahora d' un divisor cualquiera de los números n y m. Entonces

$$d' \mid n,\ d' \mid m \Rightarrow d' \mid nu_0,\ d' \mid mv_0 \Rightarrow d' \mid (nu_0 + mv_0) \Rightarrow d' \mid d.$$

Así, d posee todas las propiedades del máximo común divisor, y por eso $d =$ m.c.d. (n, m). Llegamos a la siguiente afirmación.

El máximo común divisor de dos números enteros n, m, que no se anulan conjuntamente, siempre se escribe de la forma siguiente

$$\text{m.c.d.}\ (n,\ m) = nu + mv; \quad u,\ v \in \mathbf{Z}. \tag{4}$$

En particular, los números enteros n, m, son primos entre sí cuando, y sólo cuando,

$$nu + mv = 1 \tag{4'}$$

para algunos u, $v \in \mathbf{Z}$. ■

Fue comprobado, que la condición de primos entre sí de n, m lleva a la relación (4'). Por lo contrario, si n, m son tales, que tiene lugar (4'), entonces $d \mid n$, $d \mid m \Rightarrow d \mid nu$, $d \mid mv \Rightarrow d \mid (nu + mv) \Rightarrow d \mid 1 \Rightarrow d = \pm 1$.

La demostración de las relaciones (4) y (4') es suficientemente efectiva. Es necesario tomar cualquier elemento positivo del conjunto J (véase (3)), y luego disminuirlo con ayuda del algoritmo de división, hasta que se obtiene el menor elemento, el que será el máximo común divisor.

EJERCICIOS

1. Cada número primo tiene la forma de $4k + 1$ o de $4k - 1$. Utilizando la multiplicidad del conjunto S dado en el punto 1, demostrar que el conjunto de los números primos de la forma $4k - 1$, es infinito. (*Indicación.* Para cualquier n natural, $4n! - 1$ tiene por lo menos un divisor primo p de la forma $4k - 1$, además, $p > n$).

2. Demostrar, que existen infinitamente muchos números primos de la forma $4k + 1$, basándose en la siguiente afirmación no trivial (véase el punto 1, § 2, cap. 9). Si n, $m \in \mathbf{Z}$, el m.c.d. $(n, m) = 1$, y, si p es un número primo, que divide a $n^2 + m^2$, entonces $p = 4k + 1$. (*Indicación.* Hacer $n = 2$ y $m = p_1 p_2 \ldots p_s$, donde $p_1, \ldots, p_s$ son números primos de la forma $p_i = 4k_i + 1$, distintos entre sí. Entonces, cada divisor primo p del número impar $n^2 + m^2$ tiene la forma $4k+1$, y, además, p no pertenece al conjunto $\{p_1, p_2, \ldots, p_s\}$).

3. Si el número natural n se divide exactamente en r números primos distintos $p_1, \ldots, p_r$, entonces, la cantidad de números menores que n y primos entre sí de n, es igual a

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_r}\right).$$

La función $\varphi : \mathbf{N} \to \mathbf{N}$ se llama función de Euler. Probar la voracidad de la fórmula para los valores de $\varphi(n)$, con $n \leqslant 25$ y con $n = p^m$ (véase también el punto 4, § 1, cap. 9).

4. Utilizando la fórmula binomial, demostrar por inducción sobre n, que, si p es un número primo, entonces $n^p - n$ se divide por p para cualquier $n \in \mathbf{Z}$. (*Indicación.* En caso de fracaso, se recomienda dirigirse al § 4 del cap. 4, que contiene una demostración, con el uso de «elevadas» reflexiones).

Capítulo 2

ESPACIOS LINEALES ARITMÉTICOS. MATRICES

Las matrices rectangulares, introducidas en el § 3 del cap. 1, se emplean tan frecuentemente, que con el tiempo apareció una parte independiente de las matemáticas, la *teoría de matrices*. Su proceso de formación tiene lugar hacia mediados del siglo pasado, pero su plenitud y elegancia las adquiere más tarde, junto con el desarrollo del álgebra lineal. Hasta ahora, la teoría de matrices continúa siendo un instrumento importante de investigación, bien apropiado a las necesidades prácticas y a las construcciones abstractas de las matemáticas modernas. Aquí serán expuestos los resultados más sencillos de la teoría de matrices.

El título del capítulo, probablemente, da lugar a la ilusión de que la descripción de objetos puramente algebraicos nos disponemos a cargarlos sobre los hombros de la geometría. En la práctica, sólo se trata de expresar cómoda y económicamente las propiedades de las matrices y las soluciones de los sistemas lineales en un idioma adoptado de la geometría. Los conceptos de espacio, vector, dependencia lineal, rango de un sistema, etc., que son aceptados por todos, se desarrollan exactamente en tanto, en cuanto son necesarios para nuestros fines inmediatos. A la intuición geométrica se le reserva un papel más honroso en otros cursos.

A propósito, los espacios lineales nos serán también necesarios para que sea posible hablar acerca de las aplicaciones lineales, de las cuales las matrices son satélites. Precisamente, la composición de aplicaciones (véase el punto 2, § 4, cap. 1) lleva por el camino más natural a la compresión del producto de matrices.

§ 1. ESPACIOS LINEALES ARITMÉTICOS

1. Argumentación. En relación con los sistemas de ecuaciones lineales, tuvimos que examinar filas de largo n, en las cuales se introducía distinto sentido. Eran filas $(a_{i1}, a_{i2}, \ldots, a_{in})$, $1 \leqslant i \leqslant m$, de la matriz $A = (a_{ij})$ de dimensiones $m \times n$, y de la solución $(x_1^\circ, x_2^\circ, \ldots, x_n^\circ)$ del sistema lineal con la matriz A. La reducción, en el § 3 del cap. 1, del sistema o de la matríz a una forma escalonada, incluía, además do una transformación elemental del tipo (I), dos actos importantes: multiplicación de una fila por un número, y la suma de dos filas. Las mismas operaciones pueden llevarse a cabo con las soluciones de un sistema lineal *homogéneo*. Efectivamente, si $(x_1', x_2', \ldots, x_n')$ y $(x_1'', x_2'', \ldots, x_n'')$ son dos soluciones del sistema $a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = 0$, $i = 1, 2, \ldots, m$, y α, β dos números reales cualesquiera, entonces, la fila

$$(\alpha x_1' + \beta x_1'', \alpha x_2' + \beta x_2'', \ldots, \alpha x_n' + \beta x_n'')$$

también será solución de nuestro sistema:

$$a_{i1}(\alpha x_1' + \beta x_1'') + a_{i2}(\alpha x_2' + \beta x_2'') + \ldots + a_{in}(\alpha x_n' + \beta x_n'') =$$
$$= \alpha(a_{i1}x_1' + a_{i2}x_2' + \ldots + a_{in}x_n') +$$
$$+ \beta(a_{i1}x_1'' + a_{i2}x_2'' + \ldots + a_{in}x_n'') = 0$$

Por otra parte, cualquier fila, independientemente de lo que exprese, es elemento del conjunto «universal» $\mathbb{R}^n$, potencia n-ésima del conjunto $\mathbb{R}$ de los números reales. Por eso, es deseable estudiar un objeto general, cuyas propiedades se transfirieran automáticamente a las matrices y a las soluciones de los sistemas homogéneos.

2. Definiciones fundamentales. Sea n, un número natural dado. Se denomina *espacio lineal aritmético de dimensión n sobre* $\mathbb{R}$, al conjunto $\mathbb{R}^n$ (los *vectores-filas* o, sencillamente, los *vectores*, son los elementos del mismo), considerado junto con las operaciones de suma de vectores y multiplicación de vectores por *escalares* (números reales). Los escalares se designan con letras minúsculas del alfabeto griego o del latino, y los vectores con letras latinas mayúsculas, como las matrices. En esencia, el vector $X = (x_1, x_2, \ldots, x_n)$ se puede considerar como una matriz de $1 \times n$ dimensiones. Sea $Y = (y_1, y_2, \ldots, y_n)$ otro vector, y λ un escalar. Por definición

$$X + Y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n),$$
$$\lambda X = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n).$$

El vector nulo $(0, 0, \ldots, 0)$, en adelante se indica con el símbolo corriente del cero, 0. Es más, a $\mathbb{R}^1$ se acostumbra a identificarlo con $\mathbb{R}$.

Las reglas formales de operaciones con los números reales, seguramente son conocidas por el lector, y se trasladan al $\mathbb{R}^n$. La enumeración de las mismas, aunque aburridora, da una idea exacta sobre que debe entenderse como espacio vectorial abstracto, que se estudia en un curso posterior de álgebra lineal y geometría:

ЛП$_1$: $X + Y = Y + X$, *para cualesquiera vectores* $X, Y \in \mathbb{R}^n$ (*ley conmutativa*);

ЛП$_2$: $(X + Y) + Z = X + (Y + Z)$, *para tres vectores cualesquiera* $X, Y, Z \in \mathbb{R}^n$ (*ley asociativa*);

ЛП$_3$: *Existe un vector especial* (*nulo*) 0 *tal, que* $X + 0 = X$ *para todo* $X \in \mathbb{R}^n$;

ЛП$_4$: *a cada* $X \in \mathbb{R}^n$ *le corresponde un vector opuesto* (*o contrario*) $-X$ *tal, que*

$$X + (-X) = 0;$$

ЛП$_5$: $1X = X$ *para todo* $X \in \mathbb{R}^n$;

ЛП$_6$: $(\alpha\beta)X = \alpha(\beta X)$ *para todos los* $\alpha, \beta \in \mathbb{R}$, $X \in \mathbb{R}^n$;

ЛП$_7$: $(\alpha + \beta)X = \alpha X + \beta X$ (*distributividad en relación con los escalares*);

ЛП$_8$: $\alpha(X + Y) = \alpha X + \alpha Y$ (*distributividad en relación con los vectores*).

La unicidad de los vectores 0 y $-X$, sobre las que se habla en *ЛП$_3$* y en *ЛП$_4$*, al igual que otros corolarios simples de las reglas indicadas (o axiomas, si se tiene en consideración el espacio vectorial abstracto), no vamos a deducirlas, considerándolas suficientemente transparentes.

Llamamos a $\mathbb{R}^n$ espacio de dimensión n, pero el propio concepto *de dimensión* adquiere sentido sólo al final de parágrafo, luego de una pequeña preparación. El origen del término «espacio lineal» se explica en el curso de geometría analítica, donde se establece la correspondencia biunívoca entre los puntos (vectores) del espacio, el plano cartesiano y sus coordenadas (x, y). La suma de vectores por la regla del paralelogramo, y la multiplicación de ellos por un número corresponden, precisamente, a las operaciones con vectores-filas en $\mathbb{R}^2$.

Juntamente con el espacio lineal de vectores-filas $(x_1, x_2, \ldots, x_n)$ de longitud n, se considera también el espacio lineal aritmético de *vectores-columnas* de altura n

$$\begin{Vmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{Vmatrix} = [x_1, x_2, \ldots, x_n],$$

como convinimos en expresarlos en el § 3 del cap. 1. Se comprende, que la diferencia entre ellos es puramente convencional, pero pronto nos convenceremos de que es útil disponer de ambas variantes del espacio aritmético. Del contexto, habitualmente, queda claro sobre qué vectores, filas o columnas se trata, por eso no se introduce ninguna simbólica especial.

Sea V un subconjunto no vacío en $\mathbb{R}^n$. Llamaremos a V *subespacio lineal* *) en $\mathbb{R}^n$, si

$$X, Y \in V \Rightarrow \alpha X + \beta Y \in V \qquad (1)$$

para todas las $\alpha, \beta \in \mathbb{R}$. En particular, el vector nulo siempre está contenido en V. Digamos, la agrupación de todos los vectores-filas $(x_1, \ldots, x_{n-1}, 0)$ con el componente $x_n = 0$, es un subespacio; es admitido identificarlo con $\mathbb{R}^{n-1}$. Tenemos una cadenita, como se suele decir, de subespacios dispuestos canónicamente

$$0 \subset \mathbb{R} \subset \mathbb{R}^2 \subset \ldots \subset \mathbb{R}^{n-1} \subset \mathbb{R}^n.$$

Las soluciones de la ecuación homogénea $x_1 + x_2 + \ldots + x_n = 0$ componen un subespacio en $\mathbb{R}^n$, $n > 1$, distinto de cero y de todo el espacio $\mathbb{R}^n$. Más abajo se dan otros ejemplos.

3. Combinaciones lineales. Envoltura lineal. Sean $X_1, X_2, \ldots, X_k$, vectores del espacio lineal aritmético $\mathbb{R}^n$, y $\alpha_1, \alpha_2, \ldots, \alpha_k$, escalares. El vector $X = \alpha_1 X_1 + \alpha_2 X_2 + \ldots + \alpha_k X_k$ se llama *combinación lineal* de los vectores X_i con coeficientes α_i. Por ejemplo, $(2, 3, 5, 5) - 3(1, 1, 1, 1) + 2(1, 0, -1, -1) = (1, 0, 0, 0)$. Sea, pues, $Y = \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_k X_k$ una combinación lineal de los mismos vectores X_i con coeficientes β_i,

*) Esta definición hasta ahora tiene un aspecto no muy satisfactorio, pero a final del parágrafo diremos algunas palabras en su defensa

y $\alpha, \beta \in \mathbb{R}$. Entonces

$$\alpha X + \beta Y = \alpha(\alpha_1 X_1 + \alpha_2 X_2 + \ldots + \alpha_k X_k) + \beta(\beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_k X_k) = (\alpha\alpha_1 + \beta\beta_1) X_1 + (\alpha\alpha_2 + \beta\beta_2) X_2 + \ldots + (\alpha\alpha_k + \beta\beta_k) X_k$$

de nuevo hay una combinación lineal de los vectores X_i con coeficientes $\alpha\alpha_i + \beta\beta_i$. Vemos que *el conjunto de todas las combinaciones lineales del sistema dado de vectores $X_1, X_2, \ldots, X_k$, es un subespacio lineal* en $\mathbb{R}^n$. Habitualmente se representa con el símbolo $\langle X_1, X_2, \ldots, X_k \rangle$ y se denomina *envoltura lineal* del sistema de vectores $X_1, X_2, \ldots, X_k$. Se dice también, que el espacio $\langle X_1, X_2, \ldots, X_k \rangle$ *cubre a* $X_1, X_2, \ldots, X_k$ o *está engendrado* por el sistema de vectores $X_1, X_2, \ldots, X_k$.

$S \subset \mathbb{R}^n$ se puede definir como la envoltura lineal de cualquier subconjunto, comprendiendo como $\langle S \rangle$ la agrupación de todas las combinaciones lineales de los sistemas finitos de vectores de S. Es claro que, si V es un subespacio en $\mathbb{R}^n$, entonces $\langle V \rangle = V$: cualquier combinación lineal de vectores de V pertenecen a V. En particular, $S \subset V \Rightarrow \langle S \rangle \subset V$, o sea, la envoltura lineal de $\langle S \rangle$ se puede definir como la intersección de todos los subespacios que contienen el conjunto dado de vectores S, de $\mathbb{R}^n$:

$$\langle S \rangle = \bigcap_{S \subset V} V \qquad (2)$$

A primera vista no es evidente que, lo contenido en el segundo miembro de (2), una intersección $\bigcap V$ de alguna familia de semiespacios, resultará un subespacio. Pero si $X, Y \in \bigcap V$, entonces $X, Y \in V$ para cada subespacio de V, que pertenece a esta familia. Esto significa, que $\alpha X + \beta Y \in V$ para todas las $\alpha, \beta \in \mathbb{R}$, y esto da la inclusión necesaria $\alpha X + \beta Y \in \bigcap V$.

Por el contrario, la unión $U \cup V$ de los subespacios U y V, en general, no es un subespacio, como lo muestra aunque más no sea el ejemplo de los subespacios $U = \{(\lambda, 0) \mid \lambda \in \mathbb{R}\}$, $V = \{(0, \lambda) \mid \lambda \in \mathbb{R}\}$ en $\mathbb{R}^2$. Se llama envoltura lineal $\langle U \cup V \rangle$ a la *suma* de los subespacios U y V:

$$U + V = \langle U \cup V \rangle = \{u + v \mid u \in U, v \in V\}.$$

Si $U \cap V = 0$, entonces, se dice que la suma de $U + V$ es *directa*, y se escribe $U \oplus V$. Sea $V = V_1 \oplus V_2$, y $X = X_1 + X_2 = X_1' + X_2'$, dos expresiones del vector $X \in V$, en forma de combinación lineal de los vectores $X_1, X_1' \in V_1$ y $X_2, X_2' \in V_2$. Entonces tenemos $X_1 - X_1' = X_2' - X_2 \in V_1 \cap V_2$, y como $V_1 \cap V_2 = 0$, entonces $X_1 = X_1'$, $X_2 = X_2'$. Por el contrario, si la escritura $X = X_1 + X_2$, $X_i \in V_i$, $i = 1, 2$, es única para cada vector $X \in V$, entonces, la suma $V = V_1 + V_2$ es directa (dejamos esto en calidad de ejercicio). En forma más general, la suma V de subespacios $V_1, \ldots, V_k \subset \mathbb{R}^n$ es denominada suma directa $V = V_1 \oplus \ldots \otimes V_k$, si cada vector $X \in V$ tiene expresión unívoca de la forma $X = X_1 + \ldots + X_k$ con $X_i \in V_i$.

EJEMPLO 1. Examinemos dos conjuntos en $\mathbb{R}^n$:

$$U_m = \{(\lambda_1, \ldots, \lambda_m, 0, \ldots, 0) \mid \lambda_i \in \mathbb{R}\}$$

y

$$V_m = \{(0, \ldots, 0, \lambda_{m+1}, \ldots, \lambda_n) \mid \lambda_i \in \mathbb{R}\},$$

$0 < m < n$. Se comprueba inmediatamente que U_m, V_m son subespacios en R^n, y además $U_m + V_m = R^n$ y $U_m \cap V_m = 0$. Esto significa que $R^n = U_m \otimes V_m$.

EJEMPLO 2. Consideremos en R^n el llamado *vector-fila unitario*

$$E_1 = (1, 0, \ldots, 0), \quad E_2 = (0, 1, \ldots, 0), \ldots, E_n = (0, 0, \ldots,). \quad (3)$$

Cada vector $X = (x_1, x_2, \ldots, x_n)$ se escribe unívocamente en forma $X = x_1E_1 + x_2E_2 + \ldots + X_nE_n$. Por eso

$$R^n = \langle E_1 \rangle \oplus \langle E_2 \rangle \oplus \ldots \oplus \langle E_n \rangle.$$

Los vectores-columnas unitarios los designaremos con los símbolos

$$E^{(1)} = [1, 0, \ldots, 0], \; E^{(2)} = [0, 1, \ldots, 0], \ldots, E^{(n)} = [0, 0, \ldots, 1]. \quad (3')$$

4. Dependencia lineal. El sistema de vectores $X_1, \ldots, X_k$ del espacio $\mathbb{R}^n$ se llama *linealmente dependiente*, si existen k números $\alpha_1, \alpha_2, \ldots, \alpha_k$, que no sean simultáneamente nulos, y tales que

$$\alpha_1X_1 + \alpha_2X_2 + \ldots + \alpha_kX_k = 0 \quad (4)$$

(el segundo miembro es un vector nulo). Diremos también que la dependencia lineal (4) es no trivial. Pero, si $\alpha_1X_1 + \alpha_2X_2 + \ldots + \alpha_kX_k = 0 \Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$, entonces los vectores $X_1, X_2, \ldots, X_k$ se denominan *linealmente independientes*.

El ejemplo 2 del punto 3 muestra que lo vectores unitarios $E_1, E_2, \ldots, E_n$ son linealmente independientes.

Un vector $X \neq 0$, evidentemente, es siempre linealmente independiente por cuanto $\lambda X = 0$, $X \neq 0 \Rightarrow \lambda = 0$. Luego, la propiedad del sistema $X_1, \ldots, X_k$ de ser linealmente independiente, de ningún modo está vinculada con el orden de los vectores, puesto que los sumandos α_iX_i de la igualdad (4) pueden ser permutados en forma arbitraria.

TEOREMA 1. *Tienen lugar las siguientes afirmaciones:*

(i) *un sistema de vectores* $\{X_1, \ldots, X_k\}$ con un subsistema linealmente dependiente, es linealmente dependiente;

(ii) *cualquier parte de un sistema de vectores linealmente independiente* $\{X_1, \ldots, X_k\}$, *es linealmente independiente*;

(iii) *entre los vectores linealmente dependientes* $X_1, \ldots, X_k$ *por lo menos uno es combinación lineal de los restantes*;

(iv) *si uno de los vectores* $X_1, \ldots, X_k$ *se expresa linealmente por medio de los restantes, entonces los vectores* $X_1, \ldots, X_k$ *son linealmente dependientes*;

(v) *si los vectores* $X_1, \ldots, X_k$ *son linealmente independientes, y los vectores* $X_1, \ldots, X_k, X$ *son linealmente dependientes, entonces* X *es una combinación lineal de los vectores* $X_1, \ldots, X_k$;

(vi) *si los vectores* $X_1, \ldots, X_k$ *son linealmente independientes y el vector* X_{k+1} *no puede ser expresado por medio de los mismos, entonces el sistema* $X_1, \ldots, X_k, X_{k+1}$ *es linealmente independiente.*

DEMOSTRACION. (i) Sean, por ejemplo, los primeros s vectores $X_1, \ldots, X_s$, $s < k$, linealmente dependientes, o sea,

$$\alpha_1X_1 + \ldots + \alpha_sX_s = 0,$$

donde no todos los α_i son nulos. Haciendo entonces $\alpha_{s+1} = \ldots = \alpha_k = 0$, obtenemos una dependencia lineal no trivial

$$\alpha_1 X_1 + \ldots + \alpha_s X_s + \alpha_{s+1} X_{s+1} + \ldots + \alpha_k X_k = 0.$$

La afirmación (ii) se deduce inmediatamente de (i) (razonamiento por el contrario).

(iii) Sea, por ejemplo, $\alpha_k \neq 0$ en la relación (4). Entonces

$$X_k = -\frac{\alpha_1}{\alpha_k} X_1 - \ldots - \frac{\alpha_{k-1}}{\alpha_k} X_{k-1}.$$

(iv) Sea, por ejemplo, $X_k = \beta_1 X_1 + \ldots + \beta_{k-1} X_{k-1}$. Haciendo $\alpha_1 = \beta_1, \ldots, \alpha_{k-1} = \beta_{k-1}, \alpha_k = -1$, llegamos a la relación (4) con el coeficiente $\alpha_k \neq 0$.

(v) La relación no trivial

$$\beta_1 X_1 + \ldots + \beta_k X_k + \beta X = 0$$

con $\beta \neq 0$ brinda, en virtud de (iii) todo lo necesario. Si, no obstante, $\beta = 0$, entonces $\beta_1 = \ldots = \beta_k = 0$, por cuanto $X_1, \ldots, X_k$ de acuerdo a las condiciones, son linealmente independientes.

La afirmación (vi) se deduce inmediatamente de (v). ∎

5. Base. Dimensión. Damos ahora una importante

DEFINICION. Sea V un subespacio en $\mathbb{R}^n$. El sistema de vectores $X_1, \ldots, X_r \in V$ se llama *base* para V (o en V), si es linealmente independiente y su envoltura lineal coincide con V:

$$\langle X_1, \ldots, X_r \rangle = V.$$

De las definiciones de la base y de la envoltura lineal de un sistema de vectores, se deduce que cada vector $X \in V$ se escribe de un modo único, en forma de $X = \alpha_1 X_1 + \ldots + \alpha_r X_r$. Los coeficientes $\alpha_1, \ldots, \alpha_r \in \mathbb{R}^n$ se denominan *coordenadas* del vector X en la base $X_1, \ldots, X_r$.

Como hemos visto, los vectores unitarios linealmente independientes (3) engendran a $\mathbb{R}^n$. Así que, $\{E_1, E_2, \ldots, E_n\}$ es la base del espacio $\mathbb{R}^n$. Pero esta base llamada *estándar*, está lejos de ser la única base en $\mathbb{R}^n$. Por ejemplo, los vectores

$$E_1' = E_1, \quad E_2' = E_1 + E_2,$$

$$E_3' = E_1 + E_2 + E_3, \ldots, E_n' = E_1 + E_2 + \ldots + E_n$$

también conforman base en el espacio $\mathbb{R}^n$ (compruebe esto cuidadosamente). Por otro lado, hasta ahora no es claro, si cada subespacio lineal en $\mathbb{R}^n$ tiene base, y en caso de que sí, será constante la cantidad de vectores básicos o no. La respuesta a ambas preguntas resulta afirmativa. Nuestros razonamientos se basarán en el lema siguiente.

LEMA. Sean, *V un subespacio en $\mathbb{R}^n$ con base $X_1, \ldots, X_r$, e $Y_1, Y_2, \ldots, Y_s$ un sistema de vectores linealmente independientes pertenecientes a V. Entonces, $s \leqslant r$.*

DEMOSTRACION. Como todo vector de V, $Y_1, \ldots, Y_s$ son combinaciones lineales de los vectores básicos. Sean

$$\begin{aligned} Y_1 &= a_{11}X_1 + a_{21}X_2 + \ldots + a_{r1}X_r, \\ Y_2 &= a_{12}X_1 + a_{22}X_2 + \ldots + a_{r2}X_r, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ Y_s &= a_{1s}X_1 + a_{2s}X_2 + \ldots + a_{rs}X_r, \end{aligned}$$

donde a_{ij} son escalares (siendo coordenadas de los vectores Y_j, están determinados unívocamente, pero esto hasta ahora no es esencial para nosotros). Razonamos por el contrario. Supongamos que $s > r$.

Formamos la combinación lineal de los vectores Y_j con los coeficientes de x_j:

$$\begin{aligned} x_1Y_1 + \ldots + x_sY_s = (a_{11}x_1 + a_{12}x_2 + \ldots + a_{1s}x_s)\, X_1 + \ldots \\ \ldots + (a_{r1}x_1 + a_{r2}x_2 + \ldots + a_{rs}x_s)\, X_r \end{aligned}$$

y examinemos el sistema de r ecuaciones lineales con s incógnitas:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1s}x_s &= 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{r1}x_1 + a_{r2}x_2 + \ldots + a_{rs}x_s &= 0. \end{aligned}$$

Como se supuso que $s > r$, entonces es aplicable el corolario 2 del § 3 del cap. 1, de acuerdo al cual, nuestro sistema tiene solución no nula $(x_1^\circ, x_2^\circ, \ldots, x_s^\circ)$. Llegamos a una dependencia lineal no trivial

$$x_1^\circ Y_1 + x_2^\circ Y_2 + \ldots + x_s^\circ Y_s = 0,$$

cuya existencia, sin embargo, contradice la condición del lema. Por consiguiente, $s \leqslant r$. ∎

TEOREMA 2. *Cada subespacio $V \subset \mathbb{R}^n$ posee una base finita. Todas las bases de un espacio lineal V constan de un mismo número $r \leqslant n$ de vectores (este número se llama dimensión del espacio V y se expresa con el símbolo* $\dim_{\mathbb{R}} V$, *o sencillamente* $\dim V$).

DEMOSTRACION. Si $V = 0$, entonces no hay nada que demostrar. Consideramos que $V \neq 0$. Sea que encontramos en V un sistema de vectores linealmente independiente, $X_1, \ldots, X_k$. En calidad de X_1 se puede tomar cualquier vector no nulo de V. Si la envoltura lineal $\langle X_1, \ldots, X_k\rangle$ no coincide con V, entonces elegimos en V al vector $X_{k+1} \notin \langle X_1, \ldots, X_k\rangle$. En otras palabras, X_{k+1} no es una combinación lineal de los vectores $X_1, \ldots, X_k$. Según el teorema 1 (vi), el sistema $X_1, \ldots, X_k, X_{k+1}$ es linealmente independiente. Podríamos continuar un proceso ilimitado de ampliación del sistema lineal independiente, pero todos sus vectores X_i están situados en $\mathbb{R}^n = \langle E_1, E_2, \ldots, E_n\rangle$, y por el lema recién demostrado, todo sistema linealmente independiente en $\mathbb{R}^n$ contiene no más de n vectores. Así, pues, dado un cierto $r \leqslant n$ natural, el sistema lineal

independiente $X_1, \ldots, X_k, \ldots, X_r \in V$ se vuelve *maximal*, o sea, obtenemos un sistema linealmente dependiente $X_1, \ldots, X_r, X$, cualquiera que sea el vector $X \neq 0$ de V. Por el teorema 1 (v) tendremos la inclusión $X \in \langle X_1, \ldots, X_r \rangle$. Esto significa que $V = \langle X_1, \ldots, X_r \rangle$, y los vectores $X_1, \ldots, X_r$ componen la base para V.

Supongamos ahora, que $Y_1, \ldots, Y_s$ es otra base para V. Por el lema tenemos la desigualdad $s \leqslant r$. Cambiando de lugar los sistemas $X_1, \ldots, X_r$ e $Y_1, \ldots, Y_s$, obtenemos, por el mismo lema, la desigualdad $r \leqslant s$. Así, $s = r$ y el teorema queda demostrado. ∎

Observemos ahora, aunque en esto no haya una necesidad imperiosa, que todos nuestros razonamientos del mismo modo se refirieron tanto al espacio de las filas, como al espacio de las columnas.

Así, con cada subespacio lineal V en $\mathbb{R}^n$ se asocia un número entero positivo $r \leqslant n$, al que hemos denominado dimensión V: $r = \dim V$. En particular, $\dim \mathbb{R}^n = n$. Este importante parámetro numérico del espacio, se puede caracterizar de distintos modos (véanse los ejercicios). Una de las variantes para la determinación de la dimensión se basa en el concepto de rango de un sistema de vectores. Precisamente, si $\{X_1, X_2, \ldots\}$ es algún sistema de vectores, posiblemente infinito, en el espacio lineal aritmético $\mathbb{R}^n$, entonces, como sabemos, la dimensión de la envoltura lineal $\langle X_1, X_2, \ldots \rangle$ no es superior a n. Esta dimensión se denomina *rango del sistema* $\{X_1, X_2, \ldots\}$:

$$\operatorname{rank}\{X_1, X_2, \ldots\} = \dim \langle X_1, X_2, \ldots \rangle.$$

Algunas palabras en defensa del término «subespacio lineal». Elegimos en el subespacio lineal $V \subset \mathbb{R}^n$ una base cualquiera $X_1, \ldots, X_r$. Entonces, $X = \alpha_1 X_1 + \ldots + \alpha_r X_r$ para cada $X \in V$, y el conjunto V se encuentra en mutua correspondencia unívoca con el conjunto de todas las filas coordenadas $(\alpha_1, \ldots, \alpha_r)$ de largo r (o de las columnas coordenadas $[\alpha_1, \ldots, \alpha_r]$ de altura r). Además, con esta correspondencia, la combinación lineal de vectores pasa a ser combinación lineal de filas. Por lo visto, la elección de cualquier base en V nos permite interpretar a V como un espacio vectorial aritmético $\mathbb{R}^r$, incluido de algún modo en $\mathbb{R}^n$, con $n \geqslant r$.

EJERCICIOS

1. Sean V, V_1 y V_2, subespacios en $\mathbb{R}^n$, y al mismo tiempo $V \subset V_1 + V_2$. ¿Es siempre cierto que $V = V \cap V_1 + V \cap V_2$? ¿Qué se puede decir acerca de esta relación en el caso particular en que $V_1 \subset V$?

2. Sea V, un subespacio en $\mathbb{R}^n$. Si $V = U \oplus W$ es una descomposición en una suma directa, entonces el subespacio W se llama *suplemento* de U, y U, suplemento de W en V. ¿El suplemento de U en V, está determinado unívocamente? Comparar a W con el concepto conjunto teórico de suplemento $V \setminus U$ (véase el § 5 del cap. 1).

3. Mostrar, que los vectores $X_1 = (1, 2, 3)$, $X_2 = (3, 2, 1)$ son linealmente independientes; examinar la envoltura lineal $V = \langle X_1 X_2 \rangle$; mostrar, que el vector $X = (-5, 2, 9)$ está contenido en V, y hallar sus coordenadas en la base X_1, X_2, hallar en $\mathbb{R}^3$ por lo menos un suplemento de V.

4. Mostrar, que el sistema de vectores $X_1, \ldots, X_n$ de $\mathbb{R}^n$, genera a $\mathbb{R}^n$ si, y sólo si, es linealmente independiente.

5. Mostrar, que cualquier sistema de vectores, linealmente independiente, $X_1, \ldots, X_k$ del subespacio $V \subset \mathbb{R}^n$ puede incluirse en un sistema básico para V.

6. Sean U y V, subespacios en $\mathbb{R}^n$. Demostrar que si $U \cap V = 0$, entonces $\dim (U + V) = \dim U + \dim V$.

7. Hallar el rango del sistema de vectores $(0, 1, 1)$, $(1, 0, 1)$, $(1, 1, 0)$.

§ 2. RANGO DE UNA MATRIZ

1. Regreso a las ecuaciones. En el espacio lineal aritmético de columnas de altura m, examinamos n vectores

$$A^{(j)} = [a_{1j}, a_{2j}, \ldots, a_{mj}], \quad j = 1, 2, \ldots, n,$$

y su envoltura lineal $V = \langle A^{(1)}, A^{(2)}, \ldots, A^{(n)} \rangle$. Sea dado otro vector $B = [b_1, b_2, \ldots, b_m]$. Se pregunta: pertenece B al subespacio $V \subset \mathbb{R}^m$, y si pertenece, entonces, de qué modo sus coordenadas $b_1, \ldots, b_m$ (en relación a la base estándar (3′) § 1) se expresan por medio de las coordenadas de los vectores $A^{(j)}$. En el caso en que $\dim V = n$, la segunda parte de la pregunta se refiere a los valores de las coordenadas del vector B en la base $A^{(1)}, \ldots, A^{(n)}$. Tomamos una combinación lineal de los vectores $A^{(j)}$ con coeficientes arbitrarios x_j y componemos la ecuación $x_1 A^{(1)} + \ldots + x_n A^{(n)} = B$. La forma explícita de esta ecuación

$$x_1 \begin{Vmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{Vmatrix} + x_2 \begin{Vmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{Vmatrix} + \ldots + x_n \begin{Vmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{Vmatrix} = \begin{Vmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{Vmatrix} \tag{1}$$

es sólo otra forma de escribir un sistema de m ecuaciones lineales con n incógnitas:

$$\begin{gathered} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m. \end{gathered} \tag{2}$$

Precisamente, con este sistema nos encontramos por primera vez en el § 3 del cap. 1. También allí introdujimos los conceptos de matriz simple y de matriz ampliada

$$A = \begin{Vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{Vmatrix}, \quad (A|B) \begin{Vmatrix} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{Vmatrix} \tag{3}$$

del sistema lineal (2). La primera impresión es que regresamos a la posición inicial, perdiendo el tiempo sin ganar nada. De hecho, ahora disponemos de una serie de conceptos importantes. Queda por adquirir práctica en el manejo de los mismos.

En este lugar es cómodo convenir en las designaciones. En el futuro, a fin de abreviar la escritura, frecuentemente indicaremos la suma $s_1 + s_2 + \ldots + s_n$ con el signo $\sum_{i=1}^{n} s_i$. Además, las $s_1, \ldots, s_n$, son magnitudes de naturaleza arbitraria (números, vectores-filas, etc.), para las cuales se cumplen todas las leyes de la suma de números o vectores. La regla

$$\sum_{i=1}^{n} ts_i = t\sum_{i=1}^{n} s_i, \quad \sum_{i=1}^{n} (s_i + t_i) = \sum_{i=1}^{n} s_i + \sum_{i=1}^{n} t_i$$

es suficiente comprensible, y no necesita aclaración.

Serán consideradas también *las sumas dobles*

$$\sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} = \sum_{j=1}^{n} (\sum_{i=1}^{m} a_{ij}) = \sum_{i=1}^{m} (\sum_{j=1}^{n} a_{ij}) = \sum_{i,j} a_{ij},$$

en las cuales el orden de la suma (por el primer y por el segundo índice) se puede elegir a gusto. Esto es fácil de comprender, si se disponen a las magnitudes a_{ij} en una matriz rectangular de dimensiones $m \times \times n$: somos libres de comenzar la suma de los elementos por filas o por columnas.

Otros posibles tipos de suma, serán explicados en el lugar necesario.

2. Rango de una matriz. *Llamamos espacio de columnas de la matriz* rectangular A, de dimensiones $m \times n$ (véase (3)), al arriba introducido espacio $V = \langle A^{(1)}, A^{(2)}, \ldots, A^{(n)} \rangle$, al que ahora indicaremos con el símbolo $V_v(A)$, o sencillamente V_v (la v significa vertical). A su dimensión $r_v(A) = \dim V_v$, la denominamos *rango por columnas* de la matriz A. Análogamente, se introduce *el rango por filas* de la matriz A: $r_h(A) = \dim V_h$, donde $V_h = \langle A_1, A_2, \ldots, A_m \rangle$ es un subespacio en $\mathbb{R}^n$, estirado en los vectores-filas $A_i = (a_{i1}, a_{i2}, \ldots, a_{in})$, $i = 1, 2, \ldots, m$ (h significa horizontal). En otras palabras,

$$r_v(A) = \text{rank } \{A^{(1)}, A^{(2)}, \ldots, A^{(n)}\},$$
$$r_h(A) = \text{rank } \{A_1, A_2, \ldots, A_m\}$$

son rangos de sistema de vectores-columnas y de vectores-filas, respectivamente. Por el teorema 2 del § 1, las magnitudes $r_v(A)$ y $r_h(A)$, están determinadas correctamente.

Siguiendo la definición dada en el § 3 del cap. 1, diremos que la matriz A', fue obtenida de A por medio de *una transformación elemental del tipo* (I), si $A'_s = A_t$, $A'_t = A_s$, para algún par de

índices $s \neq t$, y $A'_i = A_i$, para $i \neq s, t$. Y si $A'_i = A_i$, para todo $i \neq s$, y $A'_s = A_s + \lambda A_t$, con $s \neq t$, $\lambda \in R$, entonces decimos, que a la matriz A se le ha aplicado *una transformación elemental del tipo* (II).

Observemos, que las transformaciones elementales de ambos tipos son invertibles, o sea, que la matriz A', obtenida de A por medio de una transformación elemental, pasa de nuevo a ser A, por medio de la aplicación de otra transformación elemental del mismo tipo.

LEMA. *Si la matriz A' fue obtenida de la matriz A, mediante una sucesión finita de transformaciones elementales, entonces tienen lugar las igualdades:*

(i) $r_h(A') = r_h(A)$;

(ii) $r_v(A') = r_v(A)$.

DEMOSTRACION. Es suficiente examinar el caso, cuando A' es obtenida de A aplicando una transformación elemental (abreviado, t.e.).

(i) Como, evidentemente, $\langle A_1, \ldots, A_s, \ldots, A_t, \ldots, A_m \rangle = \langle A_1, \ldots, A_t, \ldots, A_s, \ldots, A_m \rangle$ entonces, una t.e. tipo (I) no modifica el $r_h(A)$. Luego, $A'_s = A_s + \lambda A_t \Rightarrow A_s = A'_s - \lambda A_t$ y, en consecuencia, $\langle A_1, \ldots, A_s + \lambda A_t, \ldots, A_t, \ldots, A_m \rangle = \langle A_1, \ldots, A_s, \ldots, A_t, \ldots, A_m \rangle$, tal que el $r_h(A)$ no varía y con una t.e. del tipo (II).

(ii) Sean $A'^{(j)}$, $j = 1, \ldots, n$, columnas de la matriz A'. Nos es necesario demostrar, que

$$\sum_{j=1}^{n} \lambda_j A^{(j)} = 0 \Leftrightarrow \sum_{j=1}^{n} \lambda_j A'^{(j)} = 0.$$

Entonces, cualquier sistema independiente de columnas de una matriz, incluso el maximal, deberá corresponder a un sistema independiente de columnas, con *los mismos números*, de otra matriz, con lo que se establece la igualdad $r_h(A') = r_v(A)$. Observemos además, que en virtud de la inversión de las t.e., es suficiente demostrar la implicación en un sentido. Sea, por ejemplo, $\sum_{j=1}^{n} \lambda_j A^{(j)} = 0$. Entonces, sustituyendo en (1) x_j por λ_j y todos los b_i por 0, vemos, que $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ es solución del sistema homogéneo SH, asociado con el sistema lineal (2). Por el teorema 1 del cap. 1, esta solución también la es del sistema homogéneo SH', obtenido con ayuda de t.e. del tipo (I) o (II), y que tiene a A' como su matriz. Tal como el sistema SH en forma abreviada se escribe $\sum x_j A'^{(j)} = 0$, entonces llegamos a la relación $\sum \lambda_j A'^{(j)} = 0$. ∎

El resultado fundamental de este parágrafo es la afirmación siguiente:

TEOREMA 1. *Para cualquier matriz rectangular $m \times n$, A, es cierta la igualdad $r_v(A) = r_h(A)$ (este número, sencillamente se llama rango de la matriz A, y se indica con el símbolo* rank A) .

DEMOSTRACION. Según el teorema 2 del § 3 del cap 1, con un número finito de t.e., efectuadas sobre las filas A_i, de la matriz A, se puede reducir esta matriz a una forma escalonada:

$$\bar{A} = \begin{Vmatrix} \bar{a}_{11} & \dots & \bar{a}_{1k} & \dots & \bar{a}_{1l} & \dots & \bar{a}_{1s} & \dots & \bar{a}_{1n} \\ 0 & \dots & \bar{a}_{2k} & \dots & \bar{a}_{2l} & \dots & \bar{a}_{2s} & \dots & \bar{a}_{2n} \\ 0 & \dots & 0 & \dots & \bar{a}_{3l} & \dots & \bar{a}_{3s} & \dots & \bar{a}_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & 0 & \dots & 0 & \dots & \bar{a}_{rs} & \dots & \bar{a}_{rn} \\ 0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 \end{Vmatrix} \qquad (4)$$

con $\bar{a}_{11}\bar{a}_{2k}\bar{a}_{3l} \dots \bar{a}_{rs} \neq 0$. De acuerdo con el lema

$$r_v(A) = r_v(\bar{A}), \quad r_h(A) = r_h(\bar{A}),$$

así que nos es suficiente demostrar la igualdad $r_v(\bar{A}) = r_h(\bar{A})$.

Las columnas de las matrices A y $\bar{A}$ con números 1, k, l, s, que corresponden a las incógnitas principales $x_1, x_k, x_l, \dots, x_s$ del sistema lineal (2), son llamadas *columnas básicas*. Esta terminología está plenamente justificada. Suponiendo la existencia de la relación

$$\lambda_1\bar{A}^{(1)} + \lambda_k\bar{A}^{(k)} + \lambda_l\bar{A}^{(l)} + \dots + \lambda_s\bar{A}^{(s)} = 0,$$

que une a los vectores-columnas $\bar{A}^{(1)} = [\bar{a}_{11}, 0, \dots, 0]$, $\bar{A}^{(k)} = [\bar{a}_{1k}, \bar{a}_{2k}, 0, \dots, 0]$, $\bar{A}^{(s)} = [\bar{a}_{1s}, \bar{a}_{2s}, \dots, \bar{a}_{rs}, 0, \dots, 0]$ de la matriz (4), obtenemos sucesivamente: $\lambda_s\bar{a}_{rs} = 0, \dots, \lambda_l\bar{a}_{3l} = 0$, $\lambda_k\bar{a}_{2k} = 0$, $\lambda_1\bar{a}_{11} = 0$, y tal como $\bar{a}_{11}, \bar{a}_{2k} \dots \bar{a}_{rs} \neq 0$, entonces $\lambda_1 = \lambda_k = \lambda_l = \dots = \lambda_s = 0$. Esto significa, que el rango rank $\{\bar{A}^{(1)}, A^k, \bar{A}^{(l)}, \dots, \bar{A}^{(s)}\} = r$, y que $r_v(\bar{A}) \geqslant r$. Pero el espacio $\bar{V}_v$, engendrado por las columnas de la matriz $\bar{A}$, se identifica con el espacio de las columnas de la matriz, que se obtiene de $\bar{A}$, eliminando las últimas $m - r$ filas nulas. Por eso, $r_v(\bar{A}) = \dim V_v \leqslant \dim \mathbb{R}^r = r$. La confrontación de las dos desigualdades muestra, que $r_v(\bar{A}) = r$ (la desigualdad $r_v(\bar{A}) \leqslant r$ también surge del razonamiento evidente, de que todas las columnas de la matriz $\bar{A}$ son combinaciones lineales de las columnas básicas; ejecute esto por su cuenta, en calidad de ejercicio).

Por otro lado, todas las filas no nulas de la matriz $\bar{A}$ son lineal-

mente independientes: cualquier relación hipotética

$$\lambda_1\bar{A}_1+\lambda_2\bar{A}_2+\ldots+\lambda_r\bar{A}_r=0,\ \lambda_i\in\mathbb{R},$$

como en el caso con las columnas, da sucesivamente $\lambda_i\bar{a}_{11}=0$, $\lambda_2\bar{a}_{2k}=0,\ \ldots,\ \lambda_r\bar{a}_{rs}=0$, de donde $\lambda_1=\lambda_2=\ldots=\lambda_r=0$. Así que $r_h(\bar{A})=r=r_v(\bar{A})$. ■

3. Criterio de compatibilidad. La forma escalonada de la matriz A, que da respuesta a una serie de cuestiones referentes a los sistemas lineales (véase el § 3 del cap. 1), contiene elementos de arbitrariedad, vinculados, por ejemplo, con la elección de las columnas básicas o, lo que es equivalente, con la elección de las principales incógnitas del sistema (2). Al mismo tiempo, del teorema 1 y de su demostración se extrae lo siguiente.

COROLARIO. *El número de las incógnitas principales del sistema lineal* (2), *no depende del modo con se lleve este sistema a la forma escalonada, y es igual a* rank A, *donde A es la matriz del sistema.*

Efectivamente, hemos visto que el número de incógnitas principales es igual al número de filas no nulas de la matriz $\bar{A}$ (véase (4)), coincidente, como vimos, con el rango de la matriz A. El rango es definido por nosotros de un modo totalmente invariante. Con estas palabras se expresa el hecho de que el rango de una matriz le sirve a ella de característica intrínseca, no dependiendo de cualesquiera circunstancias accesorias. ■

En el capítulo siguiente obtendremos un medio efectivo para el cálculo del rango de la matriz A, eliminando la necesidad de llevarla a la forma escalonada. Esto, indudablemente, eleva el valor de las afirmaciones basadas en el concepto de rango. En calidad de ejemplo sencillo pero útil, formulemos el criterio de resolución de un sistema lineal, acerca del cual ya se habló en el cap. 1.

TEOREMA 2. (de Kronecker—Capelli). *El sistema de ecuaciones lineales* (2) *es compatible si, y sólo si, el rango de su matriz coincide con el rango de la matriz ampliada* (véase (4)).

DEMOSTRACIÓN. La compatibilidad del sistema lineal (2), expresado en la forma (1), se puede interpretar (con esto se comenzó el presente parágrafo) como una cuestión acerca de la presentación del vector-columna B de los términos independientes en forma de combinación lineal de los vectores-columnas $A^{(j)}$ de la matriz A. Si tal presentación es posible (o sea, el sistema (2) compatible), entonces, $B\in\langle A^{(1)},\ \ldots,\ A^{(n)}\rangle$ y rank $\{A^{1},\ \ldots,\ A^{(n)}\}=$ $=$ rank $\{A^{(1)},\ \ldots,\ A^{(n)},\ B\}$, de donde rank $A=r_v(A)=$ $=r_v((A\mid B))=$ rank $(A\mid B)$ (véase la formulación del teorema 1).

Por el contrario, si los rangos de las matrices A y $(A\mid B)$ coinciden, y $\{A^{(j_1)},\ \ldots,\ A^{j_r}\}$ es algún sistema linealmente independiente maximal de las columnas básicas de la matriz A, entonces, el sistema ampliado $\{A^{(j_1)},\ \ldots,\ A^{j_r},\ B\}$, será linealmente depen-

diente, y esto, por el teorema 1 (v) del § 1, significa que B es combinación lineal de las columnas básicas (más aún, de todas) A^j. O sea, el sistema (2) es compatible. ∎

EJERCICIOS

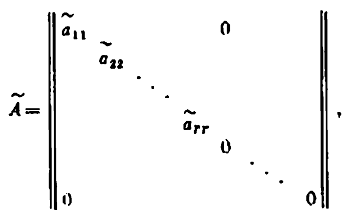
1. Demostrar el teorema 1, sin reducir la $m \times n$ — matriz $A = (a_{ij})$ a la forma escalonada. (*Indicación*. Sean, $\dim V_h(A) = r$, $\dim V_v(A) = s$. Elegir r filas básicas; sin limitación de comunidad se puede considerar que ellas son las primeras r filas $A_1, A_2, \ldots, A_r$. Examinar la $r \times n$-matriz acortada $\tilde{A} = [A_1, A_2, \ldots, A_r]$, formada por las primeras r filas de la matriz A. Elegir en $\tilde{A}$ t columnas básicas, $t = \dim V_v(\tilde{A})$. Sean ellas $\tilde{A}^{(1)}, \ldots, \tilde{A}^{(t)}$. Como $V_v(\tilde{A}) \subset K^r$, entonces $t \leqslant r$. Para cada columna $A^{(k)}$, $k > t$, es preciso hallar escalares $\lambda_1, \ldots, \lambda_t \in K$, tales que $A^{(k)} = \lambda_1 A^{(1)} + \ldots \lambda_t A^{(t)}$, o sea, $a_{ik} = \sum_{p=1}^{t} \lambda_p a_{ip}$, $1 \leqslant i \leqslant m$. Para $i \leqslant r$, esto es seguramente así, puesto que se tiene la relación $\tilde{A}^{(k)} = \lambda_1 \tilde{A}^{(1)} + \ldots + \lambda_t \tilde{A}^{(t)}$ para las columnas acortadas. Para $i > r$, utilizar la expresión $A_i = \mu_1 A_1 + \ldots + \mu_r A_r$ de la i-ésima fila por medio de las primeras r filas.

De ellas sigue que, $a_{ik} = \sum_{l=1}^{r} \mu_l a_{lk} = \sum_{l=1}^{r} \mu_l \sum_{p=1}^{t} \lambda_p a_{lp} = \sum_{p=1}^{t} \lambda_p \sum_{l=1}^{r} \mu_l a_{lp} = \sum_{p=1}^{t} \lambda_p a_{ip}$. La dependencia lineal de columnas establecida, muestra que $s \leqslant t$, y como $t \geqslant r$, entonces $s \leqslant r$. Examinar más adelante, la llamada matriz *traspuesta*

$$
{}^tA = \begin{Vmatrix} a_{11} & a_{21} & \ldots & a_{m1} \\ a_{12} & a_{22} & \ldots & a_{m2} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1n} & a_{2n} & \ldots & a_{mn} \end{Vmatrix}
$$

de dimensiones $n \times m$. Tienen lugar las igualdades $r_h({}^tA) = r_v(A)$, $r_v({}^tA) = r_h(A)$, por eso, por lo demostrado $r \leqslant s$. Así que $r = s$).

2. Como en el caso de las filas, la permutación de las columnas, con números s y t, de la matriz A, se llama transformación elemental (t. e.) del tipo (I), y la suma a la s-ésima columna, de t-ésima columna multiplicada por el escalar λ, — t.e. del tipo (II). Indicar la forma escalonada de la matriz A por columnas. Por medio de t.e. sobre las columnas, llevar a la matriz $\tilde{A}$ (véase (4)) a la forma



$$
\tilde{A} = \begin{Vmatrix} \tilde{a}_{11} & & & & & 0 \\ & \tilde{a}_{22} & & & & \\ & & \ddots & & & \\ & & & \tilde{a}_{rr} & & \\ & & & & 0 & \\ & & & & & \ddots \\ 0 & & & & & 0 \end{Vmatrix},
$$

3. Mostrar, que para $a_0 \neq 0$, la matriz cuadrada

$$A = \begin{Vmatrix} 0 & 0 & \dots & 0 & 0 & a_0 \\ 1 & 0 & \dots & 0 & 0 & a_1 \\ 0 & 1 & \dots & 0 & 0 & a_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 1 & 0 & a_{n-1} \\ 0 & 0 & \dots & 0 & 1 & a_n \end{Vmatrix}$$

tiene rango n.

4. Expresar la condición de igualdad de los rangos de las dos matrices

$$A = \begin{Vmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{Vmatrix}, \qquad B = \begin{Vmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \beta_1 & \beta_2 & \dots & \beta_n \\ \gamma_1 & \gamma_2 & \dots & \gamma_n \end{Vmatrix}$$

mediante la propiedad geométrica del conjunto de n rectas en el plano.

§ 3. APLICACIONES LINEALES. OPERACIONES CON MATRICES

1. Matrices y aplicaciones. Sean $\mathbb{R}^n$ y $\mathbb{R}^m$ dos espacios lineales aritméticos de columnas de altura n y m, respectivamente. Sea, luego, $A = (a_{ij})$ una matriz de dimensiones $m \times n$. Definimos la aplicación φ_A: $\mathbb{R}^n \to$ [redacted], suponiendo para cualquier $X = [x_1\ x_2, \dots$ $\dots, x_n] \in \mathbb{R}^n$

$$\varphi_A(X) = x_1 A^{(1)} + x_2 A^{(2)} + \dots + x_n A^{(n)}, \tag{1}$$

donde $A^{(1)}, \dots, A^{(n)}$, son columnas de la matriz A (comparar con (1) del § 2). Como ellas tienen una altura m, entonces, en el segundo miembro de (1) se encuentra el vector-columna $Y = [y_1, y_2, \dots$ $\dots, y_m] \in \mathbb{R}^m$. Explícitamente, (1) se vuelve a escribir en la forma

$$y_i = \sum_{j=1}^{n} a_{ij} x_j, \quad i = 1, 2, \dots, m. \tag{1'}$$

Si $X = X' + X'' = [x_1' + x_1'', x_2' + x_2'', \dots, x_n' + x_n'']$, entonces,

$$\varphi_A(X' + X'') = \sum_{i=1}^{n} (x_i' + x_i'') A^{(i)} = \sum_{i=1}^{n} x_i' (A)^{(i)} + \sum_{i=1}^{n} x_i'' A^{(i)} = \varphi_A(X') + \varphi_A(X'').$$

Análogamente

$$\varphi_A(\lambda X) = \sum_{i=1}^{n} \lambda x_i A^{(i)} = \lambda \sum_{i=1}^{n} x_i A^{(i)} = \lambda \varphi_A(X), \quad \lambda \in \mathbb{R}.$$

Por el contrario, supongamos que φ: $\mathbb{R}^{(n)} \to \mathbb{R}^m$ es una aplicación de los conjuntos en el sentido del § 5. del cap. 1, poseedora de las dos propiedades siguientes:

(i) *$\varphi(X' + X'') = \varphi(X') + \varphi(X'')$ para todos los X', $X'' \in \mathbb{R}^{(n)}$;*

(ii) *$\varphi(\lambda X) = \lambda \varphi(X)$ para todos los $X \in \mathbb{R}^{(n)}$, y $\lambda \in \mathbb{R}$.*

Entonces designando a las columnas básicas estándares (véase el punto 3 del § 1) de los espacios $\mathbb{R}^n$ y $\mathbb{R}^m$, correspondientemente con los símbolos $E_n^{(1)}, \ldots, E_n^{(n)}$ y $E_m^{(1)}, \ldots, E_m^{(m)}$, aprovechamos las propiedades (i) y (ii), aplicándolas al vector arbitrario

$$X = [x_1, x_2, \ldots, x_n] = \sum_{j=1}^{n} x_j E_n^{(j)} \in \mathbb{R}^n:$$

$$\varphi(X) = \varphi\left(\sum_{j=1}^{n} x_j E_n^{(j)}\right) = \sum_{j=1}^{n} x_j \varphi(E_n^{(j)}). \tag{2}$$

La relación (2) muestra que la aplicación φ se determina totalmente con sus valores, en los vectores-columnas básicos. Haciendo

$$\varphi(E_n^{(j)}) = \sum_{i=1}^{m} a_{ij} E_m^{(i)} = [a_{1j}, a_{2j}, \ldots, a_{mj}] = A^{(j)} \in \mathbb{R}^m, \tag{3}$$

descubrimos, que la φ dada es equivalente a la matriz rectangular $A = (a_{ij})$ dada, de dimensiones $m \times n$, con columnas $A^{(1)}, \ldots$ $\ldots, A^{(n)}$, y que las relaciones (1) y (2), de hecho, coinciden. Así que se puede admitir que $\varphi = \varphi_A$.

DEFINICION. La aplicación $\varphi = \varphi_A$: $\mathbb{R}^n \to \mathbb{R}^m$, poseedora de las propiedades (i) y (ii), se llama *aplicación lineal* de $\mathbb{R}^n$ en $\mathbb{R}^m$. Frecuentemente, en especial cuando $n = m$, se hace referencia a *transformaciones lineales*. La matriz A se llama *matriz de la aplicación lineal* φ_A.

Sean φ_A y $\varphi_{A'}$, dos aplicaciones lineales de $\mathbb{R}^n \to \mathbb{R}^m$ con las matrices $A = (a_{ij})$ y $A' = (a'_{ij})$. Entonces, la igualdad $\varphi_A = \varphi_{A'}$ es equivalente a la coincidencia del significado $\varphi_A(X) = \varphi_{A'}(X)$, para todos los $X \in \mathbb{R}^n$. En particular, $A'^{(j)} = \varphi_{A'}(E_n^{(j)}) =$ $= \varphi_A(E_n^{(j)}) = A^{(j)}$, $1 \leqslant j \leqslant n$, de donde $a'_{ij} = a_{ij}$ y $A' = A$.

Resumimos nuestros resultados:

TEOREMA 1. *Entre las aplicaciones lineales de* $\mathbb{R}^n$ *en* $\mathbb{R}^m$ *y las matrices de dimensiones* $m \times n$, *existe una correspondencia recíprocamente unívoca.*

Hay que subrayar, que no tiene sentido hablar de aplicaciones lineales $S \to T$ de los conjuntos arbitrarios S y T. Las condiciones (i) y (ii) presuponen que S y T son subespacios de los espacios lineales aritméticos $\mathbb{R}^n$, $\mathbb{R}^m$.

Prestemos atención al caso especial $m = 1$, cuando la aplicación lineal φ: $\mathbb{R}^n \to \mathbb{R}$, generalmente denominada *función lineal* de n variables, se da por medio de n escalares $a_1, a_2, \ldots, a_n$:

$$\varphi(X) = \varphi(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n. \tag{4}$$

Nuestra terminología se diferencia de la adoptada en la escuela media, donde (en el caso de una variable x) a la aplicación lineal la llama función $x \to ax + b$.

Las funciones lineales (4), al igual que las aplicaciones lineales arbitrarias de $\mathbb{R}^n \to \mathbb{R}^m$ con n y m dados, pueden sumarse y multi-

plicarse por escalares. De hecho, sean φ_A, φ_B: $\mathbb{R}^n \to \mathbb{R}^m$ dos aplicaciones lineales. La aplicación

$$\varphi = \alpha\varphi_A + \beta\varphi_B\colon \mathbb{R}^n \to \mathbb{R}^m,\ \alpha,\ \beta \in \mathbb{R},$$

se determina por sus valores:

$$\varphi(X) = \alpha\varphi_A(X) + \beta\varphi_B(X).$$

En el segundo miembro hay una combinación lineal corriente de vectores-columnas.

Como

$$\varphi(X' + X'') = \alpha\varphi_A(X' + X'') + \beta\varphi_B(X' + X'') =$$
$$= \alpha\{\varphi_A(X') + \varphi_A(X'')\} + \beta\{\varphi_B(X') + \varphi_B(X'')\} =$$
$$= \{\alpha\varphi_A(X') + \beta\varphi_B(X')\} + \{\alpha\varphi_A(X'') + \beta\varphi_B(X'')\} = \varphi(X') +$$
$$+ \varphi X'';\ \varphi(\lambda X) = \alpha\varphi_A(\lambda X) + \beta\varphi_B(\lambda X) = \alpha\lambda\varphi_A(X) +$$
$$+ \beta\lambda\varphi_B(X) = \lambda\{\alpha\varphi_A(X) + \beta\varphi_B(X)\} = \lambda\varphi(X)$$

(aquí, en forma no evidente usamos las reglas $ЛП_1$ — $ЛП_8$ del § 1), entonces, φ es una aplicación lineal. En virtud del teorema 1, se puede hablar de su matriz C: $\varphi = \varphi_C$. Para hallar C, copiemos, siguiendo a (3), la columna con el número j:

$$[c_{1j},\ c_{2j},\ \ldots,\ c_{mj}] = C^{(j)} = \varphi_C(E_n^{(j)}) = \alpha\varphi_A(E_n^{(j)}) + \beta\varphi_B(E_n^{(j)}) =$$
$$= \alpha A^{(j)} + \beta B^{(j)} = [\alpha a_{1j} + \beta b_{1j},\ \alpha a_{2j} + \beta b_{2j},\ \ldots,\ \alpha a_{mj} + \beta b_{mj}].$$

A la matriz $C = (c_{ij})$ con elementos $c_{ij} = \alpha a_{ij} + \beta b_{ij}$ es natural llamarla combinación lineal de las matrices A y B, con los coeficientes α y β:

$$\alpha\begin{Vmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ a_{m1} & \ldots & a_{mn} \end{Vmatrix} + \beta\begin{Vmatrix} b_{11} & \ldots & b_{1n} \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ b_{m1} & \ldots & b_{mn} \end{Vmatrix} =$$
$$= \begin{Vmatrix} \alpha a_{11} + \beta b_{11} & \ldots & \alpha a_{1n} + \beta b_{1n} \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ \alpha a_{m1} + \beta b_{m1} & \ldots & \alpha a_{mn} + \beta b_{mn} \end{Vmatrix}. \qquad (5)$$

Así,

$$\alpha\varphi_A + \beta\varphi_B = \varphi_{\alpha A + \beta B}. \qquad (6)$$

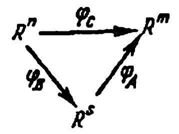
Especialmente con frecuencia utilizaremos el hecho, de que las combinaciones lineales de funciones lineales, de nuevo resultan funciones lineales.

Para finalizar este punto señalemos que, si las reglas $ЛП_1$ — $ЛП_8$ del § 1 para los espacios lineales se copian reemplazando en todas partes a los vectores-filas X, Y, Z, por matrices de dimensiones $m \times n$, entonces, en correspondencia con las relaciones determinantes (5), se obtendrán las reglas $ЛМ_1$ — $ЛМ_8$, que dan fundamento para hablar sobre un espacio lineal de matrices de dimensiones $m \times n$.

Si se desea, éste puede considerarse como una escritura compacta del espacio lineal $\mathbb{R}^{mn}$ de filas de largo mn (filas divididas en segmentos de largo n, dispuestas unas sobre otras).

2. **Rroducto de matrices.** Las relaciones (5) y (6) expresan coordinación de las operaciones de suma y multiplicación por escalares, en los conjuntos de matrices de dimensiones $m \times n$ y de aplicaciones de $\mathbb{R}^n \to \mathbb{R}^m$. En el caso de conjuntos arbitrarios se tiene otro concepto importante de producto (composición) de aplicaciones (véase el punto 2, § 5, del cap. 1). Es sensato esperar que la composición de dos aplicaciones lineales deba de expresarse de algún modo concordante en términos de matrices. Veamos como se hace esto.

Sean $\varphi_B: \mathbb{R}^n \to \mathbb{R}^s$, $\varphi_A: \mathbb{R}^s \to \mathbb{R}^m$ dos aplicaciones lineales, y $\varphi_C = \varphi_A \circ \varphi_B$ su composición:



Hablando en general, nos será necesario probar previamente que $\varphi = \varphi_A \circ \varphi_B$ es una aplicación lineal, pero esto es suficientemente claro:

(i) $\varphi(X' + X'') = \varphi_A(\varphi_B(X' + X'')) = \varphi_A(\varphi_B(X') + \varphi_B(X'')) = \varphi_A(\varphi_B(X')) + \varphi_A(\varphi_B(X'')) = \varphi(X') + \varphi(X'')$;

(ii) $\varphi(\lambda X) = \varphi_A(\varphi_B(\lambda X)) = \varphi_A(\lambda\varphi_B(X)) = \lambda\varphi_A(\varphi_B(X)) = \lambda\varphi(X)$; por eso, por el teorema 1, con φ se asocia una matriz C completamente determinada.

La operación con aplicaciones en las columnas en cadena

$$[x_1, \ldots, x_n] \overset{\varphi_B}{\longmapsto} [y_1, \ldots, y_s] \overset{\varphi_A}{\longmapsto} [z_1, \ldots, z_m]$$

la escribimos explícitamente, de acuerdo a la fórmula (1')

$$z_i = \sum_{k=1}^{s} a_{ik} y_k = \sum_{k=1}^{s} a_{ik} \sum_{j=1}^{n} b_{kj} x_j = \sum_{j=1}^{n} \Big(\sum_{k=1}^{s} a_{ik} b_{kj}\Big) x_j.$$

Por otra parte

$$z_i = \sum_{j=1}^{n} c_{ij}, \; x_j, \quad i = 1, 2, \ldots, m.$$

Comparando las expresiones obtenidas, y recordando que x_j ($j = 1, 2, \ldots, n$) son números reales arbitrarios, llegamos a las relaciones

$$c_{ij} = \sum_{k=1}^{s} a_{ik} b_{kj}, \quad 1 \leqslant i \leqslant m, \quad 1 \leqslant j \leqslant n. \tag{7}$$

Diremos, que la matriz $C = (c_{ij})$ se obtiene como resultado de *multiplicar* la matriz A por la matriz B. Es admitido escribir

$$C = AB.$$

De este modo, se denomina *producto* de la matriz rectangular (a_{ik}), de dimensiones $m \times s$, por la matriz rectangular (b_{kj}), de dimensiones $s \times n$, a la matriz rectangular (c_{ij}), de dimensiones $m \times n$, con elementos c_{ij}, dados por la relación (7). Hemos demostrado el

TEOREMA 2. *El producto $\varphi_A\varphi_B$ de dos aplicaciones lineales con matrices A y B, es una aplicación lineal con matriz $C = AB$. En otras palabras,*

$$\varphi_A\varphi_B = \varphi_{AB}. \quad \blacksquare \tag{8}$$

La relación (8) es un suplemento natural de la (6).

Nos podemos olvidar de las aplicaciones lineales, y hallar el producto AB de dos matrices arbitrarias A, B, teniendo en cuenta, sin embargo, que *el símbolo AB tiene sentido sólo en el caso cuando el número de columnas de la matriz A, coincide con el número de filas de la matriz B.* Precisamente con esta condición funciona la regla (7) de «multiplicación de la i-ésima fila A_i; por la j-ésima columna $B^{(j)}$», de acuerdo a la cual

$$c_{ij} = (a_{i1}, \ldots, a_{is})\,[b_{1j}, \ldots, b_{sj}] = A_iB^{(j)}. \tag{9}$$

El número de filas de la matriz Ab, es igual al número de filas de la matriz A, y el número de columnas, igual al número de columnas de la matriz B. En particular, el producto de matrices cuadradas de un mismo orden siempre es determinado, pero, aún en este caso, hablando en general, $AB \neq BA$, como lo muestra, aunque más no sea, el siguiente ejemplo:

$$\begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix}\begin{Vmatrix} 0 & 0 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix} \neq \begin{Vmatrix} 0 & 0 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 0 \\ 1 & 0 \end{Vmatrix}\begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix}.$$

El producto de matrices, por supuesto, se podría haber introducido de muchos otros modos (multiplicar, por ejemplo, filas por filas), pero ninguno de estos modos es comparable, por su importancia, con el examinado más arriba. Esto se entiende, por cuanto nosotros llegamos al mismo por medio del estudio de la composición natural (superposición) de aplicaciones y el propio concepto de aplicación es uno de los más fundamentales en las matemáticas.

COROLARIO. *La multiplicación de matrices es asociativa:*

$$A\,(BC) = (AB)\,C.$$

Efectivamente, el producto de matrices corresponde al producto de aplicaciones lineales (teorema 2 y relación (8)), y según el teorema 1 del § 5 del cap. 1, el producto de cualesquiera aplicaciones es asociativo. A este mismo resultado se puede llegar por el camino del cálculo, utilizando directamente la relación (7). $\blacksquare$

3. Matrices cuadradas. Sea $M_n(\mathbb{R})$ (o M_n) el conjunto de todas. La forma escalonada de la matriz las matrices cuadradas (a_{ij}), de orden n, con coeficientes reales a_{ij}.

A la transformación unitaria $e_{\mathbb{R}^n}$: $\mathbb{R}^n \to \mathbb{R}^n$, que traslada cada columna $X \in \mathbb{R}^n$ en sí misma, le corresponde, evidentemente, la matriz unidad

$$E = \left\| \begin{matrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 1 \end{matrix} \right\|.$$

Se puede escribir $E = (\delta_{kj})$, donde

$$\delta_{kj} = \begin{cases} 1, & \text{si } k = j, \\ 0, & \text{si } k \neq j, \end{cases}$$

es *el símbolo de Kronecker*. La regla (7) de multiplicación de matrices, en la cual hay que sustituir a b_{kj} por δ_{kj}, muestra que es justa la relación

$$EA = A = AE, \qquad \forall A \in M_n(\mathbb{R}). \tag{10}$$

Las relaciones matriciales (10), obtenidas por el camino del cálculo, surgen, por supuesto, de las relaciones $e\varphi = \varphi = \varphi e$ para la aplicación arbitraria φ (véase el punto 2 del § 5 del cap. 1), si se aprovechan el teorema 1 y la igualdad (8) con $\varphi_A = \varphi$, $\varphi_B = \varphi_E = e$.

Como sabemos (véase (5)), las matrices de $M_n(\mathbb{R})$ se pueden multiplicar por un número, interpretando como λA la matriz (λa_{ij}), donde $A = (a_{ij})$.

Pero la multiplicación por un escalar (número) se reduce a la multiplicación de las matrices:

$$\lambda A = \text{diag}_n(\lambda) \cdot A = A \, \text{diag}_n(\lambda), \tag{11}$$

donde

$$\text{diag}_n(\lambda) = \lambda E = \left\| \begin{matrix} \lambda & 0 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & \lambda \end{matrix} \right\|$$

es la matriz escalar conocida por nosotros (véase el § 4 del cap. 1).

En la igualdad (11) se refleja el hecho, fácilmente comprobable, de permutación de la $\text{diag}_n(\lambda)$ con cualquier matriz A. Muy importante para sus aplicaciones, resulta su siguiente tratamiento.

TEOREMA 3. *Una matriz de M_n, permutable con todas las matrices en M_n, deberá ser escalar.*

DEMOSTRACIÓN. Introducimos la matriz E_{ij}, donde, en la intersección de la i-ésima fila con la j-ésima columna está el 1, y los restantes elementos son nulos. Si $Z = (z_{ij})$ es la matriz de la que se habla en el teorema, entonces, ella es permutable, particularmen-

te, con todas las E_{ij}:

$$ZE_{ij} = E_{ij}Z, \quad i, j = 1, 2, \ldots, n.$$

Multiplicando ambos miembros de esta igualdad, obtenemos las matrices

$$\underset{\{j\}}{\left\| \begin{matrix} 0 & \ldots & z_{1i} & \ldots & 0 \\ 0 & \ldots & z_{2i} & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \ldots & z_{ni} & \ldots & 0 \end{matrix} \right\|} \quad \text{y} \quad \left\| \begin{matrix} 0 & 0 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ z_{j1} & z_{j2} & \ldots & z_{jn} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 0 \end{matrix} \right\| \{i\}$$

con la única j-ésima columna no nula y. correspondientemente, con la única i-ésima fila no nula. La comparación entre ambas inmediatamente conlleva a las relaciones $z_{ki} = 0$ para $k \neq i$ y $z_{ii} = z_{jj}$. Intercambiando i y j, obtenemos lo requerido. ∎

Notemos también las relaciones $\lambda (AB) = (\lambda A) B = A (\lambda B)$, que se deducen inmediatamente según la definición de multiplicación de matrices por escalares o, si se quiere, aplicando las relaciones (11) y mediante la propiedad asociativa de la multiplicación de matrices.

Para la matriz dada $A \in M_n (\mathbb{R})$ se puede hacer la prueba de hallar tal matriz $B \in M_n (\mathbb{R})$, que se cumpla la condición

$$AB = E = BA. \tag{12}$$

Si la matriz B existe, entonces, a la condición (12), en términos de transformaciones lineales, le responde la condición

$$\varphi_A\varphi_B = e = \varphi_B\varphi_A, \tag{12'}$$

que significa que $\varphi_B = \varphi_A^{-1}$ es una transformación inversa a φ_A. De acuerdo al teorema 2 del § 5 del cap. 1, φ_A^{-1} existe si, y sólo si, φ_A es una transformación biyectiva. Además, la φ_A^{-1} está determinada unívocamente. Como $\varphi_A (0) = 0$, entonces, la biyectividad de la φ_A significa, en particular, que

$$X \neq 0, \quad X \in \mathbb{R}^n \Rightarrow \varphi_A (X) \neq 0. \tag{13}$$

Sea ahora φ_A alguna transformación lineal biyectiva de $\mathbb{R}^n$ en $\mathbb{R}^n$. La transformación inversa a ella, φ_A^{-1}, existe, pero, hablando en general, no está claro si es o no lineal. A fin de convencerse de la linealidad de φ_A^{-1}, introducimos los vectores-columnas

$$X = \varphi_A^{-1} (X' + X'') - \varphi_A^{-1} (X') - \varphi_A^{-1} (X''),$$
$$Y = \varphi_A^{-1} (\lambda Y') - \lambda\varphi_A^{-1} (Y')$$

y aplicamos a ambos miembros de estas igualdades la transformación φ_A. En virtud de su linealidad obtenemos

$$\varphi_A(X) = \varphi_A(\varphi_A^{-1}(X' + X'')) - \varphi_A(\varphi_A^{-1}(X')) - \varphi_A(\varphi_A^{-1}(X'')),$$
$$\varphi_A(Y) = \varphi_A(\varphi_A^{-1}(\lambda Y')) - \lambda\varphi_A(\varphi_A^{-1}(Y')).$$

Como $\varphi_A\varphi_A^{-1} = e$, entonces

$$\varphi_A(X) = e(X' + X'') - e(X') - e(X'') = 0,$$
$$\varphi_A(Y) = e(\lambda Y') - \lambda e(Y') = 0,$$

de donde, en correspondencia con la implicación (13), hallamos que X, Y, son vectores nulos. De este modo, se cumplen las condiciones (i) y (ii) del punto 1, que definen a las aplicaciones lineales. Tenemos $\varphi_A^{-1} = \varphi_B$, donde B es una matriz cualquiera. Copiando la condición (12′) en forma $\varphi_{AB} = \varphi_E = \varphi_{BA}$ [véase (8)] y de nuevo empleando el teorema 1, llegamos a las igualdades (12).

Así, la *matriz, inversa a* $A \in M_n(\mathbb{R})$, *precisamente existe, entonces, cuando la transformación* $\varphi_A: \mathbb{R}^n \to \mathbb{R}^n$ *es biyectiva. Además, la transformación* φ_A^{-1} *es lineal.* La biyección de φ_A es equivalente a la condición de que cualquier vector-columna $Y \in \mathbb{R}^n$ se escribe unívocamente en forma (1)

$$Y = \varphi_A(X) = x_1A^{(1)} + x_2A^{(2)} + \ldots + x_nA^{(n)},$$

donde $A^{(1)}, A^{(2)}, \ldots, A^{(n)}$, son columnas de la matriz A (la sobreyectividad de φ_A lleva a la existencia de X, para el cual $Y = \varphi_A(X)$, y la inyectividad de φ_A muestra la unicidad de X: si $Y = \varphi_A(X') = \varphi_A(X'')$, entonces, $\varphi_A(X' - X'') = \varphi_A(X') - \varphi_A(X'') = 0$, de donde, de acuerdo a (12), $X' - X'' = 0$). Esto significa que el $\mathbb{R}^n$ coincide con el espacio de las columnas $V_v(A) = \langle A^{(1)}, \ldots, A^{(n)}\rangle$ de la matriz A, así que el rank $A = \dim \mathbb{R}^n = n$.

Si existe la matriz inversa de A, entonces, de acuerdo con lo expresado arriba, es única. Se acostumbra designarla con el símbolo A^{-1}. En tal caso (véase (12′))

$$\varphi_A^{-1} = \varphi_{A^{-1}}. \tag{14}$$

La matriz cuadrada A, para la cual existe matriz inversa A^{-1}, se denomina *no degenerada* (o *no singular*)*. También se llama no degenerada la correspondiente transformación lineal φ_A. En caso contrario, la matriz A y la transformación lineal φ_A se llaman *degeneradas* (o *singulares*).

Resumimos los resultados que hemos obtenido.

TEOREMA 4. *La matriz cuadrada* A, *de orden* n, *es no degenerada si, y sólo si, su rango es igual a* n. *La transformación* φ_A^{-1}, *inversa de* φ_A, *es lineal y está dada por la igualdad* (14). ∎

*) También se llama matriz no regular. (Nota del T.)

COROLARIO. *La no degeneración de* φ_A *lleva a la no degeneración de* φ_A^{-1}, y $(A^{-1})^{-1} = A$. *Si,* A, B, ... C, D *son matrices no degeneradas de* $n \times n$ *dimensiones, entonces, el producto* $AB \ldots CD$ también es no degenerado y $(AB \ldots CD)^{-1} = D^{-1}C^{-1} \ldots B^{-1}A^{-1}$.

Para demostrarlo es suficiente fundarse bien en el corolario del teorema 2 del § 5 del cap. 1, o bien en la simetría de la condición $AA^{-1} = E = A^{-1}A$. ∎

La fórmula explícita para A^{-1} la mostraremos en el cap. 3. Ahora solamente advertimos que el cálculo efectivo de A^{-1} para la matriz A con coeficientes numéricos, o el cálculo del producto de dos matrices, aunque sea por el método indicado al final de este capítulo, habitualmente requiere el cumplimiento de un gran número de operaciones. En la práctica nos encontramos con matrices de orden $n = 100$ o más. Si A y B son matrices tales, entonces, para el cálculo de $C = AB$, es necesario hallar n^2 elementos c_{ij} de acuerdo con la fórmula (7) [ó (9)], lo que, en cada caso, requiere $2n - 1$ multiplicaciones y sumas de números. En total es necesario realizar $(2n - 1)\, n^2$ operaciones, o sea, cerca de dos millones de operaciones cuando $n = 100$. Para las computadoras modernas esta tarea es relativamente fácil, pero las dificultades reales aparecen, si se requiere hallar la potencia A^m de la matriz A con exponente $m \geqslant 1000$. Aquí por definición $A^m = AA^{m-1}$, de hecho $A^m = A^kA^{m-k}$, $0 \leqslant k \leqslant m$, es consecuencia fácil de la asociatividad (véase el corolario del teorema 2), como esto será mostrado en el capítulo 4 en un contexto más amplio. Para calcular A^m se utilizan distintos procedimientos complementarios, basados en la especificidad de la matriz A, o bien tomados del curso de álgebra lineal. En calidad de ilustración examinemos tres ejemplos.

EJEMPLO 1. Si

$$A = \operatorname{diag}(\alpha_1, \ldots, \alpha_n) = \left\| \begin{matrix} \alpha_1 & \ldots & 0 \\ \cdot & \cdot & \cdot \\ 0 & \ldots & \alpha_n \end{matrix} \right\|,$$

entonces, evidentemente,

$$A^m = \operatorname{diag}(\alpha_1^m, \ldots, \alpha_n^m) = \left\| \begin{matrix} \alpha_1^m & \ldots & 0 \\ \cdot & \cdot & \cdot \\ 0 & \ldots & \alpha_n^m \end{matrix} \right\|.$$

EJEMPLO 2. Sea

$$A = \left\| \begin{matrix} a & c \\ 0 & b \end{matrix} \right\|.$$

Entonces la inducción sobre m muestra que,

$$A^m = \left\| \begin{matrix} a^m & c\,\dfrac{a^m - b^m}{a-b} \\ 0 & b^m \end{matrix} \right\|,$$

donde $\dfrac{a^m - b^m}{a-b} = a^{m-1} + a^{m-2}b + \ldots + ab^{m-2} + b^{m-1}$. En particular, con $a = b$, tenemos

$$\left\| \begin{matrix} a & c \\ 0 & a \end{matrix} \right\|^m = \left\| \begin{matrix} a^m & ma^{m-1}c \\ 0 & a^m \end{matrix} \right\|.$$

EJEMPLO 3. Por indicación sobre m no es difícil convencerse de que, la m-ésima potencia de la matriz

$$A=\begin{Vmatrix} 0 & 1 \\ 1 & 1 \end{Vmatrix}$$

tiene la forma

$$A^m=\begin{Vmatrix} f_{m-1} & f_m \\ f_m & f_{m+1} \end{Vmatrix}, \qquad (15)$$

donde los números enteros $f_0=0$, $f_1=1$, $f_2=1$, $f_3=2$, ... se determinan mediante relaciones recurrentes $f_{m+1}=f_m+f_{m-1}$. Estos no son otra cosa que los números de Fibonacci (véase el ejemplo 2) al final del § 3 del cap. 1).

Introducimos la matriz

$$B=\begin{Vmatrix} -\frac{\lambda_2}{5} & \frac{1}{5} \\ -\sqrt{5}\lambda_1 & \sqrt{5} \end{Vmatrix}$$

con determinante 1 (véase el § 4 del cap. 1), donde

$$\lambda_1=\frac{1+\sqrt{5}}{2}, \qquad \lambda_2=\frac{1-\sqrt{5}}{2}.$$

Un pequeño cálculo muestra que,

$$B^{-1}=\begin{Vmatrix} \sqrt{5} & -\frac{1}{5} \\ \sqrt{5}\lambda_1 & -\frac{\lambda_2}{5} \end{Vmatrix} \quad \text{y} \quad A=B^{-1}\begin{Vmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{Vmatrix}B.$$

Pero, si tres matrices cualesquiera A, B, C, de dimensiones $n\times n$, de las cuales B es no degenerada, están vinculadas por la relación $A=B^{-1}CB$, entonces

$$A^m=B^{-1}CB\cdot B^{-1}CB\cdot B^{-1}CB\ \dots\ B^{-1}CB=B^{-1}C^mB$$

(los multiplicadores interiores BB^{-1}, sustituidos por E se «redujeron»). En nuestro caso, teniendo en cuenta el ejemplo 1 y la relación (15), tenemos

$$\begin{Vmatrix} f_{m-1} & f_m \\ f_m & f_{m+1} \end{Vmatrix}=A^m=B^{-1}\begin{Vmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{Vmatrix}^m B=$$

$$=B^{-1}\begin{Vmatrix} \lambda_1^m & 0 \\ 0 & \lambda_2^m \end{Vmatrix}B=\begin{Vmatrix} \sqrt{5} & -\frac{1}{5} \\ \sqrt{5}\lambda_1 & -\frac{\lambda_2}{5} \end{Vmatrix}\cdot\begin{Vmatrix} \lambda_1^m & 0 \\ 0 & \lambda_2^m \end{Vmatrix}B=$$

$$=\begin{Vmatrix} \sqrt{5}\lambda_1^m & -\frac{\lambda_2^m}{5} \\ \sqrt{5}\lambda_1^{m+1} & -\frac{\lambda_2^{m+1}}{5} \end{Vmatrix}\begin{Vmatrix} -\frac{\lambda_2}{5} & \frac{1}{5} \\ -\sqrt{5}\lambda_1 & \sqrt{5} \end{Vmatrix}=\begin{Vmatrix} \star & \frac{1}{\sqrt{5}}(\lambda_1^m-\lambda_2^m) \\ \star & \star \end{Vmatrix}$$

(con estrellitas están indicados los términos que no nos interesan).

Comparando los coeficientes de las matrices del primer y del segundo miembro de esta igualdad, obtenemos, para el número de Fibonacci de orden m, el valor

$$f_m=\frac{\lambda_1^m-\lambda_2^m}{\sqrt{5}}=\frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^m-\left(\frac{1-\sqrt{5}}{2}\right)^m\right\}.$$

Vemos, que $f_m \sim \frac{1}{\sqrt{5}}\lambda_1^m$ para m grandes (progresión geométrica), por cuanto $\lim\limits_{m\to\infty}\left(\frac{1-\sqrt{5}}{2}\right)^m=0$.

Hemos obtenido relativamente muchas reglas de operación con matrices cuadradas de orden n. Se tienen en cuenta las reglas JIM$_1$ — — JIM$_8$ (véase la observación al final del punto 1), la propiedad asociativa (corolario del teorema 2), (10) y el teorema 4. Prestemos de nuevo atención a las llamadas *leyes distributivas*:

$$(A+B)\,C = AC + BC, \quad C\,(A+B) = CA + CB, \tag{16}$$

donde A, B, C, son matrices arbitrarias de $M_n(\mathbb{R})$.

Efectivamente, suponiendo que $A=(a_{ij})$, $B=(b_{ij})$, $C=(c_{ij})$, obtenemos para cualesquiera $i, j=1, \ldots, n$, una igualdad (se utiliza la distributividad en $\mathbb{R}$!):

$$\sum_{k=1}^{n}(a_{ik}+b_{ik})\,c_{kj}=\sum_{k=1}^{n}a_{ik}c_{kj}+\sum_{k=1}^{n}b_{ik}c_{kj},$$

de cuyo primer miembro resulta el elemento g_{ij} de la matriz $(A+B)\,C$ y de cuyo segundo miembro se tienen los elementos h_{ij} y h'_{ij} de las matrices AC y BC, respectivamente. La segunda ley distributiva (16) se comprueba en forma totalmente análoga. La necesidad de ello está fundida por la no conmutatividad del producto en $M_n(\mathbb{R})$. Las leyes distributivas

$$(\varphi+\psi)\,\xi=\varphi\xi+\psi\xi, \quad \xi\,(\varphi+\psi)=\xi\varphi+\xi\psi \tag{16'}$$

para las transformaciones lineales φ, ψ, ξ, de $\mathbb{R}^n$ en $\mathbb{R}^n$ se pueden no demostrar, haciendo hincapié en la correspondencia entre aplicaciones y matrices, pero se puede, a su vez, deducir (16) de (16′), por cuanto en el caso de las aplicaciones el razonamiento es lo mismo de fácil:

$$\begin{aligned}((\varphi+\psi)\,\xi)\,(X) &= (\varphi+\psi)\,(\xi X)=\varphi\,(\xi X)+\psi\,(\xi X)= \\ &=(\varphi\xi)\,(X)+(\psi\xi)\,(X)=(\varphi\xi+\psi\xi)\,(X), \quad X\in\mathbb{R}^n.\end{aligned}$$

EJERCICIOS

1. Dadas las aplicaciones

a) $[x_1, x_2, \ldots, x_n]\to[x_n, \ldots, x_2, x_1]$;

b) $[x_1, x_2, \ldots, x_n]\to[x_1, x_2^2, \ldots, x_n^n]$;

c) $[x_1, x_2, \ldots, x_n]\to[x_1, x_1+x_2, \ldots, x_1+x_2+\ldots x_n]$.

¿Cuáles de ellas son lineales?

2. Verificar que

$$A=\begin{Vmatrix} a & b\\ c & d\end{Vmatrix}, \quad ad-bc\neq 0 \Rightarrow A^{-1}=\frac{1}{ad-bc}\begin{Vmatrix} d & -b\\ -c & a\end{Vmatrix}.$$

En particular, $ad-bc=1 \Rightarrow A^{1}=\begin{Vmatrix} d & -b \\ -c & a \end{Vmatrix}$. ¿Existe o no A^{-1} cuando $ad-bc=0$?

3. Demostrar, que para cualquier matriz

$$A=\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$$

se cumple la relación

$$A^{2}=(a+d)A-(ad-bc)E$$

(en otras parabras, que A es «raíz» de la ecuación cuadrada $x^{2}-(a+d)x+ +(ad-bc)=0$).

4. Con $ad-bc\neq 0$ emplear la relación del ejercicio 3 para obtener la matriz inversa A^{-1}.

5. Demostrar que

$$\begin{Vmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{Vmatrix}^{m}=\begin{Vmatrix} 1 & ma & \frac{m(m-1)}{2}ab+mc \\ 0 & 1 & mb \\ 0 & 0 & 1 \end{Vmatrix},$$

Hallar para $\begin{Vmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{Vmatrix}$ la matriz inversa.

6. Verificar que

$$\begin{Vmatrix} 0 & -1 \\ 1 & -1 \end{Vmatrix}^{3}=E.$$

7. Demostrar que, si

$$\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}^{m}=0, \quad \text{entonces} \begin{Vmatrix} a & b \\ c & d \end{Vmatrix}^{2}=0.$$

8. En las aplicaciones prácticas un papel destacado juegan las matrices *de Márkov* (o *estocásticas*):

$$P=(p_{ij}) \quad p_{ij}\geqslant 0, \quad \sum_{i=1}^{n} p_{ij}=1, \quad j=1,2, \ldots, n.$$

Las aplicaciones lineales φ_p asociadas con las matrices de Márkov, habitualmente se emplean para vectores-columnas especiales, los llamados *probabilísticos* (o *de probabilidades*)

$$X=[x_1, \ldots, x_n], \quad x_i\geqslant 0, \quad \sum_{i=1}^{n} x_i=1.$$

La concordancia de estas definiciones, dictadas por problemas científico-naturales, se aprecia en las siguientes afirmaciones, las cuales es necesario demostrar aunque sólo sea para $n=2$.

a) La matriz $P\in M_n(\mathbb{R})$ es matriz de Márkov, propiamente dicha, siempre cuando junto con cualquier vector probabilístico X, el vector PX también resulta probabilístico (aquí $PX=\varphi_p(X)$),

b) Si P es una matriz de Márkov *positiva* ($p_{ij} > 0$, $\forall i, j$), entonces, a cualquier vector probabilístico X le responde un vector *positivo* probabilístico PX (todos sus componentes son rigurosamente mayores que cero).

c) Si P y Q son matrices de Márkov, entonces, también la matriz PQ será de Márkov. Esto significa, en particular, que cualquier potencia P^k de esta matriz también es matriz de Márkov.

§ 4. ESPACIO DE SOLUCIONES

1. Soluciones de un sistema lineal homogéneo. De las observaciones incorporadas a principios de los §§ 2 y 3 se deduce que el sistema de ecuaciones lineales con matriz A de dimensiones $m \times n$ y columna $B \in \mathbb{R}^m$, puede ser indicado sintéticamente en la forma

$$\varphi_A (X) = B, \qquad (1)$$

o

$$AX = B \qquad (1')$$

(en el primer miembro se tiene el producto de matrices de dimensiones $m \times n$ y $n \times 1$).

Imaginándose por un momento que $m = n$ y que la matriz cuadrada A, de orden n, no es degenerada (véase punto 3 del § 3), obtenemos una solución, además única, del sistema (1'), multiplicando ambos miembros de la relación matricial, a la izquierda, por A^{-1}: $X = EX = (A^{-1}A) X = A^{-1} (AX) = A^{-1}B$. Esta cómoda escritura simbólica de la solución del sistema cuadrado determinado, no nos libera de los cálculos, por cuanto la matriz A^{-1} no nos es previamente dada. Pero no nos privaremos de la satisfacción de observar, que el aparato matricial desarrollado en el § 3, brinda, por lo menos, un placer estético. Utilicémoslo ahora para apreciar todas las soluciones del sistema (1). Con este fin, examinemos en principio el sistema homogéneo asociado, cuando $B = [0, 0, \dots, 0] = 0$.

Se llama *núcleo* de la aplicación lineal φ_A: $\mathbb{R}^n \to \mathbb{R}^m$ al conjunto

$$\operatorname{Ker} \varphi_A = \{X \in \mathbb{R}^n \mid \varphi_A (X) = 0\}$$

(Ker del inglés *kernel*). En otras palabras, $\operatorname{Ker} \varphi_A$ es el conjunto de las soluciones del sistema homogéneo con matriz A. De hecho, $\operatorname{Ker} \varphi_A$ es un subespacio en $\mathbb{R}^n$ (denominado *espacio de soluciones del sistema lineal homogéneo*), lo que ya se señaló al principio del § 1 y que fácilmente sigue de la linealidad de la aplicación φ_A:

$$X', X'' \in \operatorname{Ker} \varphi_A \Rightarrow \varphi_A (\alpha X' + \beta X'') = $$
$$= \alpha\varphi_A (X') + \beta\varphi_A (X'') = 0 \Rightarrow \alpha X' + \beta X'' \in \operatorname{Ker} \varphi_A.$$

A su vez, la imagen $\operatorname{Im} \varphi_A$ de la aplicación φ_A es un subespacio en $\mathbb{R}^m$: si $B' = \varphi_A (X')$, $B'' = \varphi_A (X'') \in \operatorname{Im} \varphi_A$, entonces y

$$\alpha B' + \beta B'' = \alpha\varphi_A (X') + \beta\varphi_A (X'') = \varphi_A (\alpha X' + \beta X'') \in \operatorname{Im} \varphi_A.$$

La compatibilidad del sistema (1) es equivalente a que $B \in \operatorname{Im} \varphi_A$. Sean

$$s = \dim \operatorname{Ker} \varphi_A, \quad r = \dim \operatorname{Im} \varphi_A$$

las dimensiones de los espacios $\operatorname{Ker} \varphi_A$ e $\operatorname{Im} \varphi_A$. De la definición de dimensión en el § 1 se deduce, que $s \leqslant n$, $r \leqslant m$. Al mismo tiempo $r \leqslant n$, puesto que cualquier sistema linealmente independiente $\varphi_A(X^{(1)}), \ldots, \varphi_A(X^{(k)})$ en $\operatorname{Im} \varphi_A$ se puede obtener sólo a partir del sistema lineal independiente $X^{(1)}, \ldots, X^{(k)}$ en $\mathbb{R}^n$. Una información más exacta la da el

TEOREMA 1. *Tiene lugar la igualdad $r + s = n$. Luego, el número $r = \dim \operatorname{Im} \varphi_A$ coincide con el rango de la matriz A (y por esta causa r se llama rango de la aplicación lineal φ_A).*

DEMOSTRACION. Elegimos la base $X^{(1)}, \ldots, X^{(s)}$ del subespacio $\operatorname{Ker} \varphi_A \subset \mathbb{R}^n$ y completamos al mismo hasta la base $X^{(1)}, \ldots, X^{(s)}, X^{(s+1)}, \ldots, X^{(n)}$ de todo el espacio $\mathbb{R}^n$. Esto siempre se puede hacer, como lo indica la demostración del teorema 2 del § 1 (y el ejercicio 5 del § 1). Para cualquier vector $X = \sum_i \alpha_i X^{(i)} \in \mathbb{R}^n$ tenemos

$$\varphi_A(X) = \sum_{i=1}^{n} \alpha_i \varphi_A(X^{(i)}) = \alpha_{s+1}\varphi_A(X^{(s+1)}) + \ldots \alpha_n \varphi_A(X^{(n)}),$$

tal que $\operatorname{Im} \varphi_A = \langle \varphi_A(X^{(s+1)}) \ldots, \varphi_A(X^{(n)}) \rangle$ y $r \leqslant n - s$. Los vectores $\varphi_A(X^{(s+1)}), \ldots, \varphi_A(X^{(n)})$ son linealmente independientes, por cuanto de $0 = \sum_{k \geqslant s+1} \alpha_k \varphi_A(X^{(k)}) = \varphi_A\left(\sum_{k \geqslant s+1} \alpha_k X^{(k)}\right)$ sigue, que $\sum_{k \geqslant s+1} \alpha_k X^{(k)} \in \operatorname{Ker} \varphi_A$, y esto, en virtud de la elección $X^{(s+1)}, \ldots, X^{(n)}$ sólo es posible cuando $\alpha_{s+1} = \ldots = \alpha_n = 0$. O sea, $r = n - s$. Luego, por definición de φ_A para $X = [x_1, \ldots, x_n]$ tenemos $\varphi_A(X) = x A^{(1)} + \ldots + x_n A^{(n)}$, o sea, $\operatorname{Im} \varphi_A = \langle A^{(1)}, \ldots, A^{(n)} \rangle$. Pero la dimensión de la envoltura lineal $\langle A^{(1)}, \ldots, A^{(n)} \rangle$ de las columnas de la matriz A, precisamente es el rank A. ∎

Un caso particular del teorema 1 ya nos es conocido: si A es una matriz cuadrada no degenerada de orden n, entonces A y φ_A tienen un rango máximo posible n.

A fin de hallar la base del espacio de soluciones del sistema lineal homogéneo $AX = 0$ de rango r, elegimos en A r columnas básicas (el modo práctico de elección se indica en el siguiente capítulo). Con una permutación de columnas o, lo que es equivalente, con un cambio en la numeración de las variables, se puede conseguir que las columnas básicas sean las r primeras $A^{(1)}, \ldots, A^{(r)}$. Cualquier sistema de $r + 1$ columnas $A^{(1)}, \ldots, A^{(r)}, A^{(k)}$, $k > r$, será linealmente dependiente y basándose en el teorema 1 (v) del § 1, se puede

representar el sistema por medio de las relaciones:

$$x_1^{(k)}A^{(1)} + x_2^{(k)}A^{(2)} + \ldots + x_r^{(k)}A^{(r)} + A^{(k)} = 0,$$
$$k = r+1,\ r+2,\ \ldots,\ n.$$

Los vectores-columnas

$$\begin{aligned} X^{(1)} &= [x_1^{(r+1)},\ x_2^{(r+1)},\ \ldots,\ x_r^{(r+1)},\ 1,\ 0,\ \ldots,\ 0], \\ X^{(2)} &= [x_1^{(r+2)},\ x_2^{(r+2)},\ \ldots,\ x_r^{(r+2)},\ 0,\ 1,\ \ldots,\ 0], \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X^{(n-r)} &= [x_1^{(n)},\ x_2^{(n)},\ \ldots,\ x_r^{(n)},\ 0,\ 0,\ \ldots,\ 1] \end{aligned} \qquad (2)$$

en cantidad de $n - r$ son, evidentemente, linealmente independientes (a causa de la forma especial de sus últimos $n - r$ componentes) y como soluciones del sistema (1) conformarán, por el teorema 1, la base del espacio $\operatorname{Ker} \varphi_A$ de todas ellas.

Cualquier base del espacio de soluciones del sistema lineal homogéneo $AX = 0$ de rango r, se llama *sistema fundamental de soluciones*. Al sistema (2) también lo llaman sistema fundamental *normal*. De acuerdo al corolario del teorema 1 del § 2, su rango $s = \dim \operatorname{Im} \varphi_A = n - r$, es igual al número de incógnitas independientes del sistema lineal.

Un cierto sentido «geométrico» de los sistemas de ecuaciones lineales descubre la siguiente afirmación (que en adelante, no nos será necesario).

TEOREMA 2. *Todo subespacio $V \subset \mathbb{R}^n$ de dimensión s, es el espacio de soluciones de algún sistema lineal homogéneo de rango $r = n - s$.*

DEMOSTRACION. Sea $V = \langle A^{(1)}, \ldots, A^{(s)} \rangle$. Al igual que en la demostración del teorema 1, completamos el sistema lineal independiente $A^{(1)}, \ldots, A^{(s)}$ hasta la base $A^{(1)}, \ldots, A^{(s)}, A^{(s+1)}, \ldots$ $\ldots, A^{(n)}$ de todo el espacio $\mathbb{R}^n$. Cualquier vector-columna $X = [x_1, \ldots, x_n] \in \mathbb{R}^n$ se escribe unívocamente en forma

$$X = \sum_{j=1}^{n} x'_j A^{(j)} = AX', \qquad (3)$$

donde A es una matriz cuadrada de orden n, compuesta por las columnas $A^{(j)}$, y $X' = [x'_1, x'_2, \ldots, x'_n]$. Como las columnas $A^{(1)}, \ldots, A^{(n)}$, son linealmente independientes, entonces rank $A = n$ y, según el teorema 4 del § 3, existe la matriz $A^{-1} = (\bar{a}_{ij})$ inversa de A. Tenemos

$$[x'_1, \ldots, x'_n] = A^{-1}X = [\sum_{j=1}^{n} \bar{a}_{1j}x_j,\ \ldots,\ \sum_{j=1}^{n} \bar{a}_{nj}x_j].$$

El corolario del teorema 4 del § 3 muestra, que rank $A^{-1} = n$, por eso, cualesquiera r filas suyas son linealmente independientes.

Por consiguiente, el sistema homogéneo

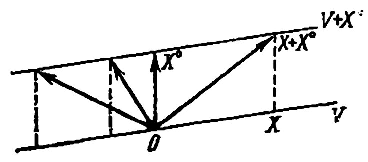
$$\sum_{j=1}^{n} \bar{a}_{kj} x_j = 0, \quad k = s+1, \ldots, n$$

tiene rango $r = n - s$. Pero el conjunto de soluciones de este sistema está compuesto, precisamente, por los vectores-columnas X del tipo (3), para los cuales $x'_{s+1} = 0, \ldots, x'_n = 0$, o sea, exactamente, por los vectores del subespacio V. ▮

2. **Multiformidades lineales. Soluciones de un sistema no homogéneo.** Sean V un subespacio en $\mathbb{R}^n$, y X° un vector perteneciente a $\mathbb{R}^n$. El conjunto

$$V + X^\circ = \{X + X^\circ \mid X \in V\} = X^\circ + V$$

se llama *multiformidad lineal* tipo V y de dimensiones dim V. La figura geométrica



ilustra esto, en general, en una forma clara: $V + X^\circ$ es el espacio V trasladado (desplazado) a la magnitud del vector X°. El subespacio V en $\mathbb{R}^n$ también es una multiformidad lineal, que responde al desplazamiento cuando el vector $X^\circ = 0$. Dos multiformidades lineales de tipo V coinciden exactamente sólo, cuando se obtienen de V al ser desplazadas a una magnitud de los vectores X', X'' tales que $X' - X'' \in V$ (la prueba de esta afirmación se le deja al lector).

En particular, si X' es un vector arbitrario de la multiformidad lineal $V + X^\circ$, entonces, $V + X'$ coincide con $V + X^\circ$.

Sean, por ejemplo, $V = \langle E^{(1)}, E^{(2)}, E^{(3)} \rangle \subset \mathbb{R}^5$, $X^\circ = [0, 0, 1, 1, 0]$, $X' = [0, 0, 0, 1, 0]$. Entonces

$$V + X^\circ = V + X' = \{[x, y, z, 1, 0] \mid x, y, z \in \mathbb{R}\}.$$

Nos dirigimos a un sistema no homogéneo de ecuaciones lineales (1). Supongamos, que el sistema (1) es compatible, o sea (según el teorema 2 del § 2), los rangos de las matrices A y $(A \mid B)$ coinciden. Sea $X^\circ = [x_1^\circ, \ldots, x_n^\circ]$ una solución cualquiera dada de este sistema, tal que $\varphi_A(X^\circ) = B$. Si X' es cualquier otra solución del sistema (1), entonces, $\varphi_A(X' - X^\circ) = \varphi_A(X') - \varphi_A(X^\circ) = B - B = 0$. O sea, la diferencia $X'' = X' - X^\circ$, entre dos soluciones del sistema no homogéneo (1), siempre es solución del sistema homogéneo correspondiente y $X' = X'' + X^\circ$. Por otra

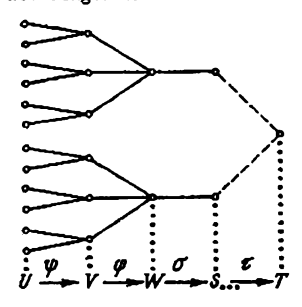
parte, si $\varphi_A(X) = 0$, entonces

$$\varphi_A(X + X^0) = \varphi_A(X) + \varphi_A(X^0) = 0 + B = B.$$

De esta manera, es cierta la siguiente afirmación.

TEOREMA 3. *Las soluciones de un sistema lineal no homogéneo compatible, llenan la multiformidad lineal del tipo V, donde $V = \operatorname{Ker} \varphi_A$, es el subespacio lineal de soluciones del sistema homogéneo correspondiente.*

3. Rango del producto de matrices. La operación de multiplicación de $\tau \ldots \sigma\varphi\psi$ aplicaciones convencionalmente se puede representar por medio del diagrama



que aclara, en el caso de aplicaciones lineales de espacios lineales, la implicación

$$\varphi\psi(U) \subset \varphi(V) \Rightarrow \operatorname{rank} \varphi\psi \leqslant \operatorname{rank} \varphi.$$

Luego, la base del espacio $\psi(U)$ se representa (como aplicación) en la base del espacio $\varphi\psi(U)$, de donde

$$\operatorname{rank} \varphi\psi \leqslant \operatorname{rank} \psi.$$

O sea,

$$\operatorname{rank} \varphi\psi \leqslant \min \{\operatorname{rank} \varphi, \operatorname{rank} \psi\}. \qquad (4)$$

Pero, $\operatorname{rank} \varphi_A = \operatorname{rank} A$, y $\operatorname{rank} AB = \operatorname{rank} \varphi_{AB} = \operatorname{rank} \varphi_A\varphi_B$, por eso, la desigualdad (4) lleva a la siguiente afirmación útil.

TEOREMA 4. *El rango del producto de matrices no es superior al rango de cada uno de los factores:*

$$\operatorname{rank} AB \leqslant \min \{\operatorname{rank} A, \operatorname{rank} B\}. \blacksquare \qquad (4')$$

COROLARIO 1. *Si B y C son matrices cuadradas no degeneradas de órdenes m y n, respectivamente, y A es una matriz arbitraria $m \times n$, entonces*

$$\operatorname{rank} BAC = \operatorname{rank} A.$$

DEMOSTRACION. Por el teorema 4 tenemos $\operatorname{rank} BAC \leqslant \operatorname{rank} BA = \operatorname{rank} BA(CC^{-1}) = \operatorname{rank} (BAC)C^{-1} \leqslant \operatorname{rank} BAC$, de donde $\operatorname{rank} BAC = \operatorname{rank} BA$. Análogamente se establece la igualdad $\operatorname{rank} BA = \operatorname{rank} A$. $\blacksquare$

COROLARIO 2. *La matriz cuadrada A de orden n, que tiene matriz inversa a la izquierda o a la derecha, no es degenerada.*

DEMOSTRACION. Supongamos que $AB = E$, para alguna matriz B de orden n. Como el rank $E = n$, entonces, la desigualdad (4′) se vuelve a escribir en forma $n \leqslant \min\{\text{rank } A, \text{ rank } B\}$, de donde se deduce, que rank A = rank $B = n$. Pero esta condición es equivalente a la no degeneración de A y B (véase el teorema 4 del § 3). Análogamente, se establece la no degeneración de A en el caso cuando existe la matriz C, para la cual $CA = E$. ∎

De acuerdo con el corolario 2, la transformación lineal φ_A: $\mathbb{R}^n \to \mathbb{R}^n$, invertible a la derecha y a la izquierda, tiene inversa de ambos lados, lo que atestigua la diferencia radical que existe entre las transformaciones lineales y las aplicaciones generales de conjuntos (véase el ejercicio 2 del § 5 del cap. 1).

4. Clases de matrices equivalentes. Al igual que en el punto 3 del § 3, designemos por medio de E_{st} a la matriz de dimensiones $m \times m$, en la cual en la intersección de la s-ésima fila con la t-ésima columna está el 1, y los restantes elementos son nulos (estas matrices a veces las llaman *matrices unidades*).

Introducimos luego en $M_m(\mathbb{R})$ las denominadas *matrices elementales*:

$$\text{(I)}\quad F_{s,t} = E - E_{ss} - E_{tt} + E_{st} + E_{ts} =$$

$$= \left\| \begin{matrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & 1 & & & \ddots & \\ & & & & & 0 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{matrix} \right\|, \quad s \neq t;$$

$$\text{(II)}\quad F_{s,t}(\lambda) = E + \lambda E_{st} = \left\| \begin{matrix} 1 & & & & \\ & \ddots & & & \\ \ldots & & 1 & \ldots\ \lambda\ \ldots & \\ & & & \ddots & \\ & & & & 1 \end{matrix} \right\|, \quad s \neq t;$$

(III) $F_s(\lambda) = E + (\lambda - 1) E_{ss} = \text{diag}\{1, \ldots, 1, \lambda, 1, \ldots, 1\}$, $\lambda \neq 0$.

Sea A una matriz arbitraria $m \times n$. Entonces, inmediatamente se comprueba, que la matriz $A' = FA$ se obtiene de A por medio de una transformación elemental (t.e) sobre las filas, del tipo (I) o (II) dependiendo de si será $F = F_{s,t}$ o $F = F_{s,t}(\lambda)$. En el caso cuando $F = F_s(\lambda)$, hablaremos de t.e. del tipo (III) (multiplicación de la s-ésima fila de A_s por λ). Análogamente, la matriz $A'' = AF$ se obtiene de A por medio de t.e. de columnas. Ya sabemos, del punto 2 del § 2 y del ejercicio 2 del § 2, que las t.e. de tipos (I) y (II), efectuadas sobre las filas y columnas de la matriz A, conllevan a ésta a una forma diagonal. Puesto que

$$\begin{Vmatrix} a_1 & & & & & & & 0 \\ & a_2 & & & & & & \\ & & \ddots & & & & & \\ & & & a_r & & & & \\ & & & & 0 & & & \\ & & & & & \ddots & & \\ 0 & & & & & & & 0 \end{Vmatrix} = F_1(a_1) F_2(a_2) \ldots F_r(a_r) \begin{Vmatrix} 1 & & & & & & & 0 \\ & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & 0 & & & \\ & & & & & \ddots & & \\ 0 & & & & & & & 0 \end{Vmatrix},$$

entonces, incorporando una t.e. del tipo (III), brinda la posibilidad de obtener de A una matriz de la forma

$$\begin{Vmatrix} E_r & 0 \\ 0 & 0 \end{Vmatrix} \tag{5}$$

(aquí los ceros significan matrices de dimensiones $r \times (n - r)$, $(m - r) \times r$ y $(m - r) \times (n - r)$). De este modo,

$$P_s P_{s-1} \ldots P_1 A Q_1 Q_2 \ldots Q_t = \begin{Vmatrix} E_r & 0 \\ 0 & 0 \end{Vmatrix}, \tag{6}$$

donde P_i (correspondientemente Q_j) es una matriz elemental de orden m (correspondientemente n). Varias veces se señaló que las operaciones elementales son invertibles. Esto concuerda con la existencia de las matrices inversas

$$(F_{s,t})^{-1} = F_{s,t},\ F_{s,t}(\lambda)^{-1} = F_{s,t}(-\lambda),\ F_s(\lambda)^{-1} = F_s(\lambda^{-1}).$$

En correspondencia con el corolario del teorema 4 del § 3, las matrices $P = P_s P_{s-1} \ldots P_1$ y $Q = Q_1 Q_2 \ldots Q_t$ también son invertibles: $P^{-1} = P_1^{-1} \ldots P_{s-1}^{-1} P_s^{-1}$, $Q^{-1} = Q_t^{-1} \ldots Q_2^{-1} Q_1^{-1}$. Hagamos notar, que P_i^{-1}, Q_j^{-1}, son matrices elementales.

Dos matrices A, B de dimensiones $m \times n$, se llaman *equivalentes* y se escriben $A \sim B$, si se hallan matrices no degeneradas, de orden m y n, correspondientemente tales, que $B = PAQ$.

Como es fácil comprender, $\sim$ es relación de equivalencia: (i) $A \sim \sim A$ $(P = E_m, Q = E_n)$; (ii) $A \sim B \Rightarrow B \sim A$, por cuanto $B = = PAQ \Rightarrow A = P^{-1}BQ^{-1}$; (iii) $B = P'AQ', C = P''BQ'' \Rightarrow C = PAQ$, donde $P = P''P'$, $Q = Q'Q''$. De acuerdo con los principios generales (véase el § 6 del cap. 1), el conjunto de todas las $m \times n$ matrices se parte en relación de equivalencia $\sim$ en clases disjuntas de matrices equivalentes. Como los rangos de las matrices equivalentes son iguales (véase el corolario 1 del teorema 4), entonces, el razonamiento que nos llevó a la igualdad (6), muestra que, en calidad de representantes de las clases, se pueden tomar matrices (5). Obtenemos la siguiente afirmación.

TEOREMA 5 *El conjunto de matrices de dimensiones $m \times n$ se parte en $P = \min(m, n) + 1$ clases de equivalencias. Todas las matrices de rango r van a parar a una clase con los representantes de* (5). ∎

COROLARIO *Toda matriz $n \times n$ no degenerada, se escribe en forma de producto de matrices elementales.*

Efectivamente, todas las matrices no degeneradas de orden n pertenecen a una clase con representantes que son matrices unidades, por cuanto sus rangos son iguales a n. La relación (6)

$$P_s P_{s-1} \ldots P_1 A Q_1 Q_2 \ldots Q_t = E,$$

vuelta a escribir en forma

$$A = P_1^{-1} \ldots P_{s-1}^{-1} P_s^{-1} Q_t^{-1} \ldots Q_2^{-1} Q_1^{-1}, \qquad (7)$$

brinda la afirmación necesaria. ∎

No se afirma que la escritura de A en forma de producto de matrices elementales es única, pero, el sólo hecho que exista tal escritura es sumamente útil. En particular, se puede utilizar en la búsqueda de la matriz inversa. De hecho, de (7) hallamos:

$$A^{-1} = Q_1 Q_2 \ldots Q_t P_s P_{s-1} \ldots P_1 = QP.$$

Puesto que, a cada una de las matrices P_i, Q_j, le corresponde una transformación elemental, entonces, la cadena de transformaciones

$$\begin{aligned} E \mid A \to P_1 \mid P_1 A \to \ldots \to P_s \ldots P_1 \mid P_s \ldots \\ \ldots P_1 A \to P_s \ldots P_1 \mid P_s \ldots P_1 A Q_1 \mid Q_1 \to \ldots \\ \ldots \to P_s \ldots P_1 \mid P_s \ldots P_1 A Q_1 \ldots Q_t \mid Q_1 \ldots Q_t \end{aligned}$$

es realmente factible, aunque el número $s + t$ de todas las transformaciones puede ser grande. Los productos que nos interesan están separados por trazos ondulados para recordar que son los resultados de las transformaciones elementales sobre las filas (en la parte izquierda) y sobre las columnas (en la parte derecha) de la matriz unidad. Para $r < n$ llegamos a la conclusión, de que A es una matriz degenerada y no tiene inversa. Con $r = n$, nos queda

multiplicar Q por P, a fin de obtener A^{-1}. Notemos que el orden de las transformaciones sobre las filas y sobre las columnas se puede cambiar.

Examinemos dos ejemplos.
Para la matriz

$$A=\begin{Vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{Vmatrix}$$

tenemos

$$E\begin{Vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{Vmatrix} \to F_{2,1}(-4)\begin{Vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 7 & 8 & 9 \end{Vmatrix} \to$$

$$\to F_{3,1}(-7)\,F_{2,1}(-4)\begin{Vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{Vmatrix} \to$$

$$\to F_{3,2}(-2)\cdot F_{3,1}(-7)\,F_{2,1}(-4)\begin{Vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{Vmatrix}.$$

Como en el segundo miembro hay una matriz escalonada de rango 2, entonces, rank $A = 2$. En consecuencia, A es una matriz degenerada.

De la cadena

$$E\begin{Vmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{Vmatrix} \to F_{1,2}\begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{Vmatrix} \to$$

$$\to F_{2,3}F_{1,2}\begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{Vmatrix} \to F_{3,4}F_{2,3}F_{1,2}\begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{Vmatrix}$$

hallamos

$$\begin{Vmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{Vmatrix}^{-1} = F_{3,4}F_{2,3}F_{1,2} = \begin{Vmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{Vmatrix}$$

en la práctica, los productos $F_{2,3}F_{1,2}$, $F_{3,4}F_{2,3}F_{1,2}$ inmediatamente se hubiesen expresado explícitamente).

El cálculo de la matriz inversa por el nuevo método, llamado a veces *(P, Q)-reducción de la matriz a la forma normal* (5), es suficientemente cómodo, aunque es temprano para hablar sobre sus

ventajas e insuficiencias basándose en los sencillos ejemplos examinados: no nos fueron necesarias, incluso, todas las transformaciones $F_{s,t}$, $F_{s,t}(\lambda)$, $F_s(\lambda)$.

EJERCICIOS

1. Obtener las reglas de operaciones con las matrices traspuestas (ver ejercicio 1 del § 2)

$$^t(A+B) = {}^tA + {}^tB;$$
$$^t(AB) = {}^tB \cdot {}^tA.$$

2. Demostrar, por razonamientos directos con las matrices, que rank $AB \leqslant \min\{\text{rank } A, \text{rank } B\}$. (*Indicación*: Prestar atención a que, si en la matriz B, son bases las columnas con números $j_1, \ldots, j_r$, entonces, todas las columnas de la matriz AB se expresan linealmente por medio de las columnas $(AB)^{(k)}$, $k = j_1, \ldots, j_r$. Lo mismo se refiere a la matriz traspuesta $^t(AB) = {}^tB{}^tA$.)

3. Demostrar *la desigualdad de Sylvester*

$$\dim \operatorname{Ker} \varphi\psi \leqslant \dim \operatorname{Ker} \varphi + \dim \operatorname{Ker} \psi$$

para dos aplicaciones lineales cualesquiera $\mathbb{R}^n \xrightarrow{\psi} \mathbb{R}^m \xrightarrow{\varphi} \mathbb{R}^l$. (*Indicación*. Examinar la restricción $\bar{\varphi} = \varphi|_V$ de la aplicación φ en cualquier subespacio $V \supset \mathbb{R}^m$. Evidentemente Ker $\bar{\varphi} \subset$ Ker φ. Por consiguiente, según el teorema 1 (ya sabemos, que V se puede interpretar como $\mathbb{R}^k$, $k \leqslant m$, por eso el teorema 1 es aplicable) $\dim V - \text{rank } \bar{\varphi} = \dim \operatorname{Ker} \bar{\varphi} \leqslant \dim \operatorname{Ker} \varphi$, de donde, $\dim V - \dim \varphi(V) \leqslant \dim \operatorname{Ker} \varphi$. Haciendo $V = \psi(\mathbb{R}^n) = \operatorname{Im} \psi$, obtenemos definitivamente: $\dim \operatorname{Ker} \varphi\psi = n - \text{rank } \varphi\psi = (n - \text{rank } \psi) + (\dim V - \text{rank } \bar{\varphi}) \leqslant \dim \operatorname{Ker} \psi + \dim \operatorname{Ker} \varphi$).

4. Demostrar, que toda aplicación lineal $\varphi\colon \mathbb{R}^n \to \mathbb{R}^m$ de rango r, se escribe en forma de suma $\varphi = \varphi_1 + \ldots + \varphi_r$ de las aplicaciones φ_i de rango 1.

5. Hallar el rango de la matriz

$$A = \begin{Vmatrix} x_1y_1 & x_1y_2 & \ldots & x_1y_n \\ x_2y_1 & x_2y_2 & \ldots & x_2y_n \\ \ldots & \ldots & \ldots & \ldots \\ x_ny_1 & x_ny_2 & \ldots & x_ny_n \end{Vmatrix}.$$

(*Indicación*. Mostrar, que $A = [x_1, \ldots, x_n] (y_1, \ldots, y_n)$.)

Capítulo 3

DETERMINANTES

Las fórmulas (3) y (9) del § 4 del cap. 1, para las resoluciones de sistemas lineales cuadrados de órdenes $n = 2, 3$, inducen a pensar sobre la existencia de fórmulas semejantes para cualquier n.

A fin de cuentas, se trata de la interpretación correcta, en cada una de estas fórmulas, del numerador y del denominador. Las miraremos como los valores de alguna función «universal» det: $M_n(\mathbb{R}) \to \mathbb{R}$ del conjunto de matrices cuadradas de orden n en $\mathbb{R}$. La conformación efectiva de la función det (determinante) también da respuesta a muchas otras cuestiones sobre matrices, formuladas en el cap. 2. En efecto, el papel de la teoría de determinantes en las matemáticas es mucho más amplio que los temas tratados por nosotros, y cada una de las aplicaciones de esta teoría, indican caminos propios para su formulación. Uno de los enfoques más naturales es el geométrico, basado en la analogía «determinantes de matrices—volúmenes de figuras polidimensionales» (véase el ejercicio del § 4 del cap. 1) y en las n-formas externas. Como para esto se necesita un poquito más de geometría, nos quedaremos en el camino «analítico»*.

§ 1. DETERMINANTES: CONSTRUCCION Y PROPIEDADES PRINCIPALES

1. Construcción por el método de inducción completa. Consideraremos, que el determinante 1×1 de la matriz (a_{11}) es igual al número a_{11}. El determinante de la matriz de dimensiones 2×2 y 3×3 son introducidos, respectivamente, por las fórmulas (2) y (8) del § 4 del cap. 1. En el último caso, el determinante de la matriz 2×2 se dejó premeditadamente «sin desarrollar». Por eso mismo se subraya la base de la inducción que nos disponemos a usar para la construcción de determinantes de matrices $n \times n$.

Sea, que los determinantes de las matrices de órdenes $1, 2, \ldots, n-1$ ya han sido introducidos. Llamamos *determinante de la matriz* $A = (a_{ij})_1^n$ a la magnitud

$$D = a_{11}D_1 - a_{21}D_2 + \ldots + (-1)^{n-1}a_{n1}D_n, \qquad (1')$$

*) Formas analíticas de exposición de la teoría de determinantes, hay varias. En este capítulo al igual que en el § 4 del cap. 1, nos atenemos a las lecciones de I. R. Shafarévich (profesor de la Universidad de Moscú), suponiendo, que un ejercicio de más, por el método de inducción es útil por sí mismo. En todo caso, prácticamente, los principales modos para calcular los determinantes de matrices se obtienen bastante rápido, aunque, posiblemente, la exposición basada en la fórmula de «desarrollo completo del determinante» (véase § 3 del cap. 4) sea un poco más sencilla en A. G. Kurosch. Curso de álgebra superior, Ed. «Mir», Moscú, 1977.

donde D_k es el determinante de la matriz de orden $n-1$:

$$\begin{Vmatrix} a_{12} & \dots & a_{1n} \\ \cdot & \cdot & \cdot \\ a_{k-1,2} & \dots & a_{k-1,n} \\ a_{k+1,2} & \dots & a_{k+1,n} \\ \cdot & \cdot & \cdot \\ a_{n2} & \dots & a_{nn} \end{Vmatrix}$$

que se obtiene de A tachando la primera columna y la k-ésima fila.

Es fácil convencerse de que la expresión (1), cuando $n = 2, 3$, concuerda con las expresiones (2), (8) del § 4 del cap. 1. El determinante de la matriz $A = (a_{ij})$ se designa con el símbolo $|A|$, o también por medio de $|a_{ij}|_1^n$ o det A. Los trazos verticales se usan preferentemente, cuando la matriz A se escribe explícitamente.

Si en la matriz A se tachan la i-ésima fila y la j-ésima columna y se deja la misma disposición de los elementos restantes, entonces, se obtiene una matriz cuadrada de $(n-1)$-ésimo orden. Su determinante se indica por medio de M_{ij} y se llama *menor* de la matriz A, correspondiente al elemento a_{ij}.

Con las nuevas designaciones, la fórmula (1') adquiere la forma

$$\det A = a_{11}M_{11} - a_{21}M_{21} + \dots + (-1)^{n-1}a_{n1}M_{n1}. \quad (1)$$

En palabras, se expresa así: *se considera determinante de una matriz cuadrada de n-ésimo orden, a la suma algebraica de los productos de los elementos de la primera columna, por los menores correspondientes, además, los productos se toman con signos alternados.*

Si en lugar de la primera columna se toma la k-ésima, y los menores M_{i1} se sustituyen por los M_{ik}, entonces, como veremos más adelante, se obtiene una expresión que, a lo sumo, se diferencia del det A en el signo.

En adelante, al igual que en el cap. 2, los símbolos

$$A_i = (a_{i1}, a_{i2}, \dots, a_{in}) \quad i = 1, 2, \dots, n,$$
$$A^{(j)} = [a_{1j}, a_{2j}, \dots, a_{nj}], \quad j = 1, 2, \dots, n,$$

indicarán, respectivamente, la i-ésima fila y la j-ésima columna de la matriz $A = (a_{ij})$. La propia matriz A se representa, bien como unión de sus filas:

$$A = [A_1, A_2, \dots, A_n]$$

(columnas de filas), o bien como unión de sus columnas:

$$A = (A^{(1)}, A^{(2)}, \dots, A^{(n)})$$

(fila de columnas). Convengamos en adelante en llamar, a las filas y columnas de la $n \times n$-matriz A también *filas* y *columnas del determinante* $|a_{ij}|$ *de orden* n.

De acuerdo con la definición, $| \ | = \det$, es una función, que confronta a la matriz cuadrada A, algún número $|A| = \det A$. Nuestra tarea, es estudiar el comportamiento de esta función cuando varían las filas o las columnas de la matriz A, consideradas como elementos (vectores) del espacio lineal $\mathbb{R}^n$. Si se quiere, para nosotros, $\det A$ es la designación sintética (en el espíritu del punto 2, del § 5 cap. 1) de la función

$$\det [A_1, \ldots, A_n] \quad \text{o} \quad \det \ (A^{(1)}, \ldots, A^{(n)})$$

de n variables, que son vectores de $\mathbb{R}^n$.

A la función arbitraria $\mathscr{D}$: $[A_1, \ldots, A_n] \to \mathscr{D}(A_1, \ldots, A_n)$ la llamaremos *multilineal*, si ella es lineal para cada argumento A_i, o sea

$$\mathscr{D}(A_1, \ldots, \alpha A_i' + \beta A_i'', \ldots, A_n) = \\ = \alpha \mathscr{D}(A_1, \ldots, A_i', \ldots, A_n) + \beta \mathscr{D}(A_1, \ldots, A_i'', \ldots, A_n)$$

(comparar con el punto 1, § 3 del cap. 2). La misma función se llama *antisimétrica*, si

$$\mathscr{D}(A_1, \ldots, A_i, A_{i+1}, \ldots, A_n) = \\ = -\mathscr{D}(A_1, \ldots, A_{i+1}, A_i, \ldots, A_n) \quad 1 \leqslant i \leqslant n-1. \tag{2}$$

OBSERVACION 1. De la definición de funciones lineales (véase (4) del § 3, cap. 2) se puede concluir, que la función $\mathscr{D}$ es multilineal precisamente entonces, cuando, siendo fijas
$A_1, \ldots, A_{i-1}, A_{i+1}, \ldots, A_n$ y cuando $A_i = X = (x_1, \ldots, x_n)$
tenemos

$$\mathscr{D}(A_1, \ldots, A_n) = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

donde $\alpha_1, \ldots, \alpha_n$ son escalares, no dependientes de $x_1, \ldots, x_n$.

OBSERVACION 2. La relación antisimétrica de la función multilineal $\mathscr{D}$ es equivalente al cumplimiento de la relación

$$\mathscr{D}(A_1, \ldots, A_{i-1}, X, X, A_{i+2}, \ldots, A_n) = 0, \\ 1 \leqslant i \leqslant n-1 \tag{2'}$$

En efecto, haciendo $A_i = A_{i+1} = X$ en (2), llegamos a (2'). Por el contrario, con $X = A_i + A_{i+1}$, de (2') se deduce, en virtud de la multilinealidad de $\mathscr{D}$, la relación

$$\mathscr{D}(\ldots, A_i, A_i, \ldots) + \mathscr{D}(\ldots, A_{i+1}, A_{i+1}, \ldots) + \\ + \mathscr{D}(\ldots, A_i, A_{i+1}, \ldots) + \mathscr{D}(\ldots, A_{i+1}, A_i, \ldots) = \\ = \mathscr{D}(\ldots, A_i + A_{i+1}, A_i + A_{i+1}, \ldots) = 0.$$

Los primeros dos términos son nulos (hacer en (2'), respectivamente, $X = A_i$ y $X = A_{i+1}$), por eso es nula la suma de los dos últimos términos, lo que es sólo otra escritura de la relación (2).

Las mismas definiciones y observaciones se refieren a la función $\mathscr{D}(A^{(1)}, \ldots, A^{(n)})$ de vectores-columnas. Más aún, la condición (2)

de relación antisimétrica es aplicable a cualquier función $\mathscr{D}$: $M^{(n)} \to \mathbb{R}$, donde $M^{(n)}$ es una potencia cartesiana de algún conjunto M.

En adelante tendremos necesidad del

LEMA 1. *Al permutar de lugar dos argumentos cualesquiera de una función antisimétrica, ésta cambia su signo.*

DEMOSTRACION. Sean permutados los i-ésimo y j-ésimo argumentos, siendo $i < j$. Efectuamos una inducción para un número $k = j - i - 1$ de argumentos, entre el par permutado. Cuando $k = 0$ la afirmación del lema coincide con la definición de la función antisimétrica. Sea que el lema se cumple para todos los $j - i - 1 < k$. Entonces

$$\begin{aligned}\mathscr{D}(\ldots, X_i, X_{i+1}, \ldots, X_{j-1}, X_j, \ldots) &= \\ = -\mathscr{D}(\ldots, X_{i+1}, X_i, \ldots, X_{j-1}, X_j, \ldots) &= \\ = \mathscr{D}(\ldots, X_{i+1}, X_j, \ldots, X_{j-1}, X_i, \ldots) &= \\ = -\mathscr{D}(\ldots, X_j, X_{i+1}, \ldots, X_{j-1}, X_i, \ldots).&\blacksquare\end{aligned}$$

2. Propiedades principales de los determinantes. El concepto de determinante, introducido por nosotros, hasta ahora no es efectivo. Nos queda por obtener una serie de propiedades de los determinantes (más exactamente, funciones det), cómodas, tanto desde el punto de vista teórico, como para el cálculo.

La relación trivial $\det (a + b) = \det a + \det b$ para determinantes de primer orden, puede llevar a una conclusión falsa, de que aquella se cumple para los determinantes de orden n (mostrar un ejemplo cuando $n = 2$). El caso de $n = 2$, sugiere una interpretación más exacta de la relación examinada:

$$\begin{aligned}\begin{vmatrix} \alpha x_1' + \beta x_1'' & \alpha x_2' + \beta x_2'' \\ a_{21} & a_{22} \end{vmatrix} &= (\alpha x_1' + \beta x_1'')\alpha_{22} - (\alpha x_2' + \beta x_2'') a_{21} = \\ &= \alpha (x_1' a_{22} - x_2' a_{21}) + \beta (x_1'' a_{22} - x_2'' a_{21}) = \\ &= \alpha \begin{vmatrix} x_1' & x_2' \\ a_{21} & a_{22} \end{vmatrix} + \beta \begin{vmatrix} x_1'' & x_2'' \\ a_{21} & a_{22} \end{vmatrix}.\end{aligned}$$

De nuevo observamos, que

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = -\begin{vmatrix} a_{21} & a_{22} \\ a_{11} & a_{12} \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$$

De este modo, existe fundamento para suponer que es veraz el

TEOREMA 1. *La función $A \mapsto \det A$ en el conjunto $M_n(\mathbb{R})$, tiene las siguientes propiedades:*

D1. $\det A$ *es una función multilineal de las filas de la matriz A, o sea, el determinante de la matriz es función lineal de los elementos de cualquier fila A_i.*

D2. det A *es una función antisimétrica de la fila de la matriz* A *(en otras palabras, el determinante es nulo, si algunas de sus filas vecinas coinciden).*

D3. det $E = 1$.

DEMOSTRACION. Utilizamos la inducción sobre n. Para $n = 1, 2$, las propiedades D1 — D3 están comprobadas. Consideraremos que las tienen todos los determinantes de orden $<n$. Demostremos D1-D3 para un determinante de orden n, a partir de la fórmula (1). Comenzamos por la propiedad D3.

D3. Si

$$A = E = \begin{Vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{Vmatrix},$$

entonces, en la fórmula (1) será $a_{i1} = 0$ para $i \neq 1$ y $a_{11} = 1$, por eso, det $E = M_{11}$. El determinante M_{11} tiene la misma estructura que el det E, pero su orden es igual a $n - 1$. Por presupuesto de la inducción, podemos considerar que $M_{11} = 1$ y, por consiguiente, det $E = 1$.

Las propiedades D1, D2 las demostramos en una situación un poco más general, descrita por el siguiente lema.

LEMA 2. *Sea* $\mathcal{D}_j$: $M_n(\mathbb{R}) \to \mathbb{R}$, *una función expresada por la fórmula*

$$\mathcal{D}_j(A) = a_{1j}M_{1j} - a_{2j}M_{2j} + \dots + (-1)^{n-1}a_{nj}M_{nj} \qquad (3)$$

(por presupuesto de la inducción, todos los determinantes M_{kj} *de orden* $n - 1$ *nos son conocidos, por eso la función* $\mathcal{D}_j$ *está correctamente dada).*

Entonces, tienen lugar las afirmaciones:

D_j1. $\mathcal{D}_j$ *es una función multilineal de las filas de la matriz* A;

D_j2. $\mathcal{D}_j$ *es una función antisimétrica de las filas de la matriz* A.

DEMOSTRACION. D_j1. A fin de destacar el carácter variable de los elementos de la i-ésima fila, hacemos $x_s = a_{is}$, $s = 1, \dots, n$:

$$A = \begin{Vmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i-1,1} & \dots & a_{i-1,j} & \dots & a_{i-1,n} \\ x_1 & \dots & x_j & \dots & x_n \\ a_{i+1,1} & \dots & a_{i+1,j} & \dots & a_{i+1,n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nn} \end{Vmatrix}$$

El menor M_{ij} no depende de $x_1, \dots, x_n$, así que $\alpha_j = (-1)^{i-1}M_{ij}$ es una constante. Cualquier otro menor M_{kj}, $k \neq i$, contiene, en

calidad de una de sus filas, a $(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$, y todas sus filas restantes son constantes. Por presupuesto de la inducción, M_{kj} es función lineal de las variables $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n$, o sea, de acuerdo a la observación 1,

$$M_{kj} = \sum_{s \neq j} a_{ks} x_s, \quad k \neq i.$$

Haciendo ahora $\alpha_s = \sum_{k \neq i} (-1)^{k-i} \alpha_{ks} a_{kj}$, $s \neq j$, llegamos a la expresión

$$\mathscr{D}_j(A) = \sum_{k=1}^{n} (-1)^{k-i} a_{kj} M_{kj} =$$

$$= \alpha_j x_j + \sum_{k \neq i} (-1)^{k-i} a_{kj} \sum_{s \neq j} a_{ks} x_s =$$

$$= \alpha_j x_j + \sum_{s \neq j} \Big(\sum_{k \neq i} (-1)^{k-i} \alpha_{ks} a_{kj} \Big) x_s = \sum_{s=1}^{n} \alpha_s x_s,$$

que significa, que $\mathscr{D}_j(A)$ es función lineal de los elementos $x_1, \ldots$ $\ldots, x_n$ de la i-ésima fila de la matriz A.

D$_j$2. En correspondencia con la observación 2 del punto 2, es más cómodo demostrar la igualdad $\mathscr{D}_j(A) = 0$ para la matriz

$$A = \begin{Vmatrix} a_{11} & \ldots & a_{1j} & \ldots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ x_1 & \ldots & x_j & \ldots & x_n \\ x_1 & \ldots & x_j & \ldots & x_n \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \ldots & a_{nj} & \ldots & a_{nn} \end{Vmatrix}$$

con dos filas iguales $A_i = A_{i+1} = (x_1, \ldots, x_j, \ldots, x_n)$. El menor M_{kj}, $k \neq i, i+1$, también contiene dos filas vecinas iguales $(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$ de largo $n-1$. Por eso, por presupuesto de la inducción $M_{kj} = 0$, $k \neq i, i+1$. La fórmula (3) se vuelve a escribir en la forma

$$\mathscr{D}_j(A) = (-1)^{i-1} x_j M_{ij} + (-1)^i x_j M_{i+1\, j}.$$

Pero, evidentemente, $M_{i,\, j} = M_{i+1\, j}$. Así que

$$\mathscr{D}_j(A) = (-1)^{i-1} x_j (M_{ij} - M_{i+1,\, j}) = 0. \blacksquare$$

Haciendo $j = 1$ en la fórmula (3), y comparando la expresión obtenida con la fórmula (1), llegamos a la igualdad

$$\mathscr{D}_1(A) = \det A. \qquad (4)$$

En consecuencia, las propiedades D1, D2 de los determinantes están contenidas en la afirmación del lema. El teorema 1 queda demostrado. $\blacksquare$

Describamos más detalladamente la propiedad D1:

D1'. det $[A_1, \ldots, \lambda A_i, \ldots, A_n] = \lambda$ det $[A_1, \ldots, A_i, \ldots$ $\ldots, A_n]$, *o sea, al multiplicar alguna fila* A_i *del determinante por* λ, *el propio determinante queda multiplicado por* λ. *En particular, multiplicando a todas las filas por* λ, *obtenemos*

$$\det \lambda A = \lambda^n \det A.$$

D1''. *Si para alguna* i, *todos los elementos de* A_i *tienen la forma* $a_{ij} = a'_j + a''_j$, *entonces*, $\det A = \det A' + \det A''$, *donde* $A'_j = A''_j = A_j$ *para* $j \neq i$, *y* $A'_i = (a'_1, \ldots, a'_n)$, $A''_i = (a''_1, \ldots, a''_n)$.

Del teorema 1 surgen varias afirmaciones sencillas, que formulamos en forma de propiedades de los determinantes, pero que demostraremos para cualquier función $\mathscr{D}_j$, definida por la fórmula (3). El paso a los determinantes es provisto por la igualdad (4).

D4. *Un determinante con una fila nula, es nulo.*

Sea, por ejemplo, $A_i = (0, 0, \ldots, 0)$. Entonces, y $2A_i = (0, \ldots, 0)$. En consecuencia, por D_j1:

$$\begin{aligned} \mathscr{D}_j(A) &= \mathscr{D}_j(A_1, \ldots, A_i, \ldots, A_n) = \\ &= \mathscr{D}_j(A_1, \ldots, 2A_i, \ldots, A_n) = \\ &= 2D_j(A_1, \ldots, A_i, \ldots, A_n) = 2\mathscr{D}_j(A), \end{aligned}$$

de donde, $\mathscr{D}_j(A) = 0$. ▌

D5. *Al permutar cualesquiera dos filas (y no sólo vecinas), el determinante cambia su signo por el contrario.*

Para cualquier función $\mathscr{D}_j(A)$, esta propiedad surge de D_j2 y del lema 1. ▌

D6. *Si en la matriz cuadrada A dos filas coinciden, entonces, su determinante es nulo.*

Tomamos de nuevo una función arbitraria $\mathscr{D}_j(A)$. Intercambiando de lugar las dos filas coincidentes A_s, A_t, en A, obtenemos la misma matriz A. Por otro lado, de acuerdo a la propiedad D5 (más exactamente, la propiedad D_j5 para $\mathscr{D}_j$), $\mathscr{D}_j(A)$ toma el signo contrario. Así, $D_j(A) = -D_j(A)$, de donde $2\mathscr{D}_j(A) = 0$ y $\mathscr{D}_j(A) = 0$. ▌

D7. *Un determinante no varía, si sobre sus filas se efectúan transformaciones elementales del tipo* (II).

Es suficiente examinar el caso cuando se emplea una sola transformación elemental. Por ejemplo, al sumarle a la s-ésima fila de la matriz A su t-ésima fila multiplicada por λ, se obtuvo la matriz A'. Entonces, en correspondencia con las propiedades D1 y D6 (más exactamente, D_j1 y D_j6, para $\mathscr{D}_j$) tenemos

$$\begin{aligned} \mathscr{D}_j(A') &= \mathscr{D}_j(A_1, \ldots, A_s + \lambda A_t, \ldots, A_n) = \\ &= \mathscr{D}_j(\ldots, A_s, \ldots) + \lambda D_j(\ldots, A_t, \ldots, A_t, \ldots) \\ &= \mathscr{D}_j(A_1, \ldots, A_n) = \mathscr{D}_j(A). \end{aligned}$$ ▌

Las propiedades demostradas permiten calcular, en forma relativamente fácil, un determinante de orden n. Uno de los métodos consiste en lo siguiente. La matriz $A = (a_{ij})$ se debe reducir, por medio de transformaciones elementales, a una forma triangular (véase § 3 del cap. 1). Sea que obtenemos la matriz

$$\bar{A} = \begin{Vmatrix} \bar{a}_{11} & \bar{a}_{12} & \dots & \bar{a}_{1n} \\ 0 & \bar{a}_{22} & \dots & \bar{a}_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & \bar{a}_{nn} \end{Vmatrix}. \qquad (5)$$

Supongamos, que en el proceso de reducción fueron realizadas q transformaciones elementales del tipo (I), y alguna cantidad de transformaciones del tipo (II). Como las últimas no modifican el determinante (propiedad D7), y cada transformación del tipo (I) lo multiplica por (-1), entonces, $\det \bar{A} = (-1)^q \det A$*). Demostraremos que

$$\det \bar{A} = \bar{a}_{11}\bar{a}_{22} \dots \bar{a}_{nn}.$$

En ese caso

$$\det A = (-1)^q \bar{a}_{11}\bar{a}_{22} \dots \bar{a}_{nn}. \qquad (6)$$

Esta será una de las fórmulas para el cálculo de $\det A$.

Demostremos la fórmula para $\det \bar{A}$ por inducción sobre n. Como $\bar{a}_{21} = \dots = \bar{a}_{n1} = 0$, entonces, de acuerdo a (1), $\det \bar{A} = \bar{a}_{11}\bar{M}_{11}$, donde

$$\bar{M}_{11} = \begin{vmatrix} \bar{a}_{22} & \bar{a}_{23} & \dots & \bar{a}_{2n} \\ 0 & \bar{a}_{33} & \dots & \bar{a}_{3n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & \bar{a}_{nn} \end{vmatrix}$$

es un determinante de orden $n-1$. Por presupuesto de la inducción $\bar{M}_{11} = \bar{a}_{22}\bar{a}_{33} \dots \bar{a}_{nn}$. Por eso, $\det \bar{A} = \bar{a}_{11}\bar{M}_{11} = \bar{a}_{11}\bar{a}_{22} \dots \bar{a}_{nn}$.

Ahora, apoyándonos en la fórmula (6), estableceremos un importante hecho, que concierne al papel de las propiedades D1-D3 de los determinantes. Precisamente, tiene lugar el

TEOREMA 2. *Sea $\mathscr{D}$: $M_n(\mathbb{R}) \to \mathscr{D}$, una función que tiene las siguientes propiedades:*

(i) *$\mathscr{D}(A)$ es función lineal de los elementos de cada fila de la matriz $A \in M_n(\mathbb{R})$;*

---

*) Hay que hacer notar, que hubiésemos podido reducir la matriz A a una forma escalonada, con ayuda de transformaciones elementales (sobre las filas) del tipo (II) solamente, que no cambian el signo del determinante, entonces, en la demostración no habría necesidad de usar el multiplicador $(-1)^q$.

(ii) *cuando se permutan dos filas vecinas,* $\mathscr{D}(A)$ *cambia de signo (en otras palabras,* $\mathscr{D}(A)$ *es función multilineal y antisimétrica de las filas de la matriz).*

Entonces, existe una constante ρ, *no dependiente de* A, *tal que*

$$\mathscr{D}(A) = \rho \cdot \det A.$$

El número ρ *se determina de la relación* $\rho = \mathscr{D}(E)$, *donde* E *es una matriz unidad.*

DEMOSTRACIÓN. Según el lema 1 $\mathscr{D}(A)$ cambia de signo al permutar dos filas cualesquiera, o sea, con cualquier transformación elemental del tipo (I). Luego, un razonamiento análogo al efectuado para demostrar la propiedad D7, muestra, que $\mathscr{D}(A)$ no varía, si las filas de la matriz A se someten a una transformación elemental del tipo (II).

Reducimos la matriz A, con ayuda de transformaciones elementales, a la forma triangular (5), donde, claro que algunos de los $\bar{a}_{ii}$ pueden ser nulos. Teniendo en cuenta lo dicho anteriormente, tenemos dos fórmulas

$$\det A = (-1)^q \det \bar{A} = (-1)^q \bar{a}_{11}\bar{a}_{22} \ldots \bar{a}_{nn} \text{ (ver (6))},$$

$$\mathscr{D}(A) = (-1)^q \mathscr{D}(\bar{A}),$$

donde q es el número de transformaciones elementales del tipo (I), efectuadas durante el paso de A a $\bar{A}$. La igualdad que necesitamos $\mathscr{D}(A) = \rho \cdot \det A$ es, evidentemente, consecuencia de la fórmula

$$\mathscr{D}(A) = \mathscr{D}(E) \cdot \bar{a}_{11} \ldots \bar{a}_{nn}, \tag{7}$$

que ahora demostraremos (hablando con propiedad, (6) es consecuencia de (7), por cuanto, para $\mathscr{D} = \det$, en virtud de la propiedad D3 será $\mathscr{D}(E) = 1$).

De acuerdo a la condición (i) del teorema, podemos sacar al $\bar{a}_{nn}$ fuera del signo $\mathscr{D}$:

$$\mathscr{D}(\bar{A}) = \bar{a}_{nn}\mathscr{D}\left(\begin{Vmatrix} \bar{a}_{11} & \ldots & \bar{a}_{1,n-1} & \bar{a}_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \ldots & \bar{a}_{n-1,n-1} & \bar{a}_{n-1,n} \\ 0 & \ldots & 0 & 1 \end{Vmatrix}\right).$$

Le aplicamos ahora a $\bar{A}$ una transformación elemental del tipo (II): restamos de la i-ésima fila, que se encuentra bajo el signo de $\mathscr{D}$, de la matriz, la última fila, previamente multiplicada por $\bar{a}_{in}$. Con esto, los elementos de la última columna se anulan (excepto $\bar{a}_{nn} = 1$), y los restantes elementos de la matriz no sufren cambios. Aplicamos el mismo razonamiento a la penúltima fila de la nueva matriz obtenida, y así sucesivamente. Cada vez, el siguiente ele-

mento $\bar{a}_{ii}$ se saca fuera del signo $\mathscr{D}$ y el razonamiento se repite. Ejecutándolo n veces, nos convencemos de que

$$\mathscr{D}(A)=\bar{a}_{nn}\ \dots\ \bar{a}_{11}\cdot\mathscr{D}\left(\left\|\begin{matrix}1 & \dots & 0\\ \cdot & \cdot\ \cdot & \cdot\\ 0 & \dots & 1\end{matrix}\right\|\right),$$

y esto es la fórmula (7). $\blacksquare$

Así, las propiedades D1—D3 caracterizan unívocamente a la función det. Por esta razón, las consideramos propiedades básicas de los determinantes. Desde un principio se podría haber llamado determinante a la función $\mathscr{D}$, poseedora de las propiedades D1—D3, pero, en ese caso, es necesario establecer su existencia. En nuestro caso, la existencia está provista por la propia construcción de la función det, por la formula (1).

Teniendo en cuenta la futura aplicación del teorema 2, no incluimos en su formulación la condición normativa $\mathscr{D}(E) = 1$.

EJERCICIOS

1. Utilizando la fórmula (1) y la regla de los signos en el desarrollo de un determinante de tercer orden (ejercicio 1 del § 4 del cap. 1), escribir íntegramente todos los productos que entran en el desarrollo de un determinante de cuarto orden. Prestar atención al número total de términos en el desarrollo y hacer la prueba de hallar la regularidad en la distribución de los signos.

2. En el segundo miembro de la fórmula (1) hay n sumandos. A su vez, cada menor M_{i1} se indica en forma de combinación lineal de sus $n-1$ menores de orden $n-2$, y así sucesivamente. En total, en el desarrollo de un determinante det (a_{ij}) de orden n entran $n(n-1)\ \dots\ 3\cdot 2\cdot 1 = n!$ (ene factorial) productos del tipo $a_{i_1 1}a_{i_2 2}\ \dots\ a_{i_n n}$ con signo $+$ ó $-$. Mostrar que

$$\det(a_{ij})=a_{11}a_{22}\ \dots\ a_{nn}+(-1)^{\frac{n(n-1)}{2}}a_{n1}a_{n-1,\,2}\ \dots\ a_{1n}+\dots$$

3. En base a las observaciones del ejercicio anterior, empleadas respecto al determinante det (a_{ij}) con $a_{ij}=1$, para $i,\ j = 1,\ 2,\ \dots,\ n$, mostrar, que en el desarrollo de cualquier determinante de orden n, exactamente la mitad de los productos $a_{i_1 1}a_{i_2 2}\ \dots\ a_{i_n n}$ entran con signo $+$.

4. A la función antisimétrica $\Delta = R^3 \to R'$ de tres variables $x,\ y,\ z$:

$$\Delta(x,\ y,\ z) = (y-x)(z-x)(z-y)$$

escribirla en forma de determinante de tercer orden.

§ 2. PROPIEDADES ULTERIORES DE LOS DETERMINANTES

1. Desarrollo de un determinante por cualquier columna. Estamos ahora en condiciones de contestar a la pregunta que involuntariamente surgió al construir la función det: ¿juega o no la primera columna un papel especial en la fórmula recurrente (1) para el determinante de n-ésimo orden? La respuesta está contenida en la

fórmula siguiente:

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} M_{ij}. \qquad (1)$$

Para la demostración, es suficiente aplicar el teorema 2 del § 1 a la función $\mathscr{D}_j$ del lema 2 del § 1. Obtenemos la relación

$$\mathscr{D}_j(A) = \mathscr{D}_j(E)\cdot\det A.$$

Pero, de acuerdo con la fórmula (3) del § 1, $\mathscr{D}_j(E) = (-1)^{j-1}$. O sea, $\mathscr{D}_j(A) = (-1)^{j-1} \det A$. Luego de multiplicar ambos miembros de esta igualdad por $(-1)^{j-1}$ nos queda $\det A = (-1)^{j-1}\mathscr{D}_j(A)$, que sólo es otra escritura de la fórmula (1). Esta expresión se vuelve más simétrica si introducimos el llamado *complemento algebraico* $A_{ij} = (-1)^{i+j} M_{ij}$ del elemento a_{ij} del determinante A. Formulemos el resultado obtenido.

TEOREMA 1. *El determinante de la matriz A es igual a la suma de los productos de alguna fila por sus complementos algebraicos*

$$\det A = \sum_{i=1}^{n} a_{ij} A_{ij}. \ \blacksquare \qquad (2)$$

En esta afirmación todas las columnas ya juegan igual papel. Cuando $j = 1$ ella se transforma en el desarrollo inicial (1) del § 1, introductorio del concepto de determinante. Acerca de las fórmulas (1) y (2) se dice, que ellas brindan el *desarrollo de un determinante por su j-ésima columna.*

Aparece la tentación de comparar a (2) con la suma análoga por el segundo índice: $\sum_{j=1}^{n} a_{ij} A_{ij}$. Pronto, veremos que se obtiene el mismo significado del $\det A$.

2. Propiedades de los determinantes respecto a las columnas. Empleando el teorema 1, podemos obtener toda una serie de nuevas propiedades de los determinantes.

TEOREMA 2. *Las propiedades* D1—D7 *del* § 1, *se cumplen no sólo para las filas, sino que también para las columnas de los determinantes.*

DEMOSTRACION. Como fue convenido al principio, $\det A = \det [A_1, \ldots, A_n] = \det (A^{(1)}, \ldots, A^{(n)})$. Del § 1 se ve, que las propiedades D4-D7 son totalmente consecuencias formales de las propiedades D1-D3, y, por consiguiente, demostrando sus analogías para las columnas, automáticamente obtenemos las restantes propiedades en relación a las columnas. Pero la propiedad normativa D3 ocupa un lugar especial y no se refiere ni a las filas ni a las columnas. De este modo, nos quedan por examinar las propiedades D1 y D2. Las demostraremos por inducción según el orden n del determinante.

Partiremos de la fórmula (2). Ella directamente muestra, que el det A es función lineal de los elementos de la j-ésima columna, por cuanto los complementos algebraicos A_{ij} no dependen de estos elementos. Por eso mismo, la propiedad 1 queda demostrada.

Demostremos la propiedad D2, es decir la antisimetría de la función det $(A^{(1)}, \ldots, A^{(n)})$. Para $n = 1$ la propiedad D2 carece de contenido. Para $n = 2$ es fácil comprobarla inmediatamente:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc = -\begin{vmatrix} b & a \\ d & c \end{vmatrix}.$$

Sea $n > 2$. Supongamos que se permutan las columnas $A^{(k)}$ y $A^{(k+1)}$. Utilizamos la fórmula (2) con $j \neq k, k + 1$. En el menor M_{ij} (o en el complemento algebraico A_{ij}) se contienen ambas columnas $A^{(k)}$, $A^{(k+1)}$, pero en forma acortada: sin los elementos a_{ik}, $a_{i,k+1}$. Por presupuesto de la inducción, al permutar dos columnas, cada menor cambia de signo. Por lo tanto, también

$$\det(\ldots, A^{(k)}, A^{(k+1)}, \ldots) = -\det(\ldots, A^{(k+1)}, A^{(k)}, \ldots). \blacksquare$$

3. Transposición de un determinate. Recordemos el concepto introducido en el ejercicio 1 del § 2 del cap. 2. La matriz rectangular de dimensiones $n \times m$, en la que su i-ésima columna, $i = 1, 2, \ldots$ $\ldots, m$, coincide con la i-ésima fila de la matriz A de dimensiones $m \times n$, se llama *matriz traspuesta* de A. La matriz traspuesta de A se anota por medio de ${}^tA$ o de A'. En consecuencia, si $A = (a_{ij})$, ${}^tA = (a'_{ij})$, entonces $a'_{ij} = a_{ij}$. Así
La columna se puede considerar como una fila traspuesta

$${}^t\begin{Vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{Vmatrix} \begin{Vmatrix} 1 & 5 \\ 2 & 6 \\ 3 & 7 \\ 4 & 8 \end{Vmatrix},$$

La columna se puede considerar como una fila traspuesta

$$[x_1, \ldots, x_n] = {}^t(x_1, \ldots, x_n).$$

En el caso de matrices cuadradas se dice también que el determinante

$$\det{}^t A = \begin{vmatrix} a_{11} & a_{21} & \ldots & a_{n1} \\ a_{12} & a_{22} & \ldots & a_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1n} & a_{n2} & \ldots & a_{nn} \end{vmatrix}$$

se obtuvo por *trasposición del determinante* det A. Explícitamente la operación de trasposición de una matriz (determinante) de orden n, se puede presentar en forma de giro de la matriz (determinante) alrededor de un eje inmóvil, su diagonal principal. El giro alrededor de la segunda diagonal (no principal) es mucho menos usado.

TEOREMA 3. *El determinante de la matriz traspuesta coincide con el determinante de la matriz inicial*

$$\det {}^tA = \det A.$$

DEMOSTRACION. Examinemos la función $\mathscr{D}$: $M_n(\mathbb{R}) \to \mathbb{R}$, que es composición $A \mapsto {}^tA \mapsto \det {}^tA$ de la función de traslado a la matriz traspuesta y a la función det. La función $\mathscr{D}$ posee las propiedades (i), (ii), formuladas en el teorema 2 del § 1. En realidad, por el recién demostrado teorema 2, la función ${}^tA \mapsto \det {}^tA$ posee las propiedades D1-D7 respecto a las columnas de la matriz ${}^tA$, o sea, respecto a las filas de la matriz A. De este modo, $\mathscr{D}$ es función multilineal y antisimétrica de las filas de la matriz. Por el teorema 2 del § 1 tenemos $\mathscr{D}(A) = \mathscr{D}(E)\cdot\det A = \det {}^tE\cdot\det A$. Pero, ${}^tE = E$, y por eso, $\det E = 1$. Luego, $\mathscr{D}(A) = \det A$. ∎

En correspondencia con el teorema 3, las filas y las columnas de un determinante gozan los mismos derechos: las propiedades, expresadas en términos de sus filas, también se expresan en términos de sus columnas, y viceversa. Por ejemplo, juntamente con el teorema 1 sobre el desarrollo de un determinante por sus columnas, es correcto el

TEOREMA 1'. *El determinante de la matriz A es igual a la suma de los productos de todos los elementos de cualquier fila dada, por sus complementos algebraicos:*

$$\det A = \sum_{j=1}^{n} a_{ij}A_{ij}. \ \blacksquare$$

A esto se le puede agregar el criterio siguiente: *si alguna fila (alguna columna) del determinante det A, es combinación lineal de las filas restantes (columnas restantes), entonces, det A* $= 0$ (véanse las propiedades D1', D1'' y sus análogas para las columnas).

Los dos ejemplos siguientes sirven para ilustrar las propiedades obtenidas de los determinantes.

EJEMPLO 1. El determinante

$$\Delta_n = \begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_n \\ x_1^2 & x_2^2 & x_n^2 \\ \dots & \dots & \dots \\ x_1^{n-1} & x_2^{n-1} & x_n^{n-1} \end{vmatrix} = \Delta(x_1, x_2, \dots, x_n).$$

vinculado con el nombre de Vandermonde, se cualcula por la fórmula

$$\Delta_n = \prod_{1 \le i < j \le n} (x_j - x_i), \qquad (3)$$

o, en una escritura más detallada

$$\Delta_n = (x_2 - x_1)(x_3 - x_1)\dots(x_n - x_1)(x_3 - x_2)\dots(x_n - x_2)\dots$$
$$\dots(x_n - x_{n-1})$$

En particular, cuando los elementos son distintos de dos en dos $x_1, \ldots, x_n$ *el determinante de Vandermonde* es diferente de cero. Esta propiedad se utiliza frecuentemente. Por el teorema 3 también tenemos

$$\Delta_n = \begin{vmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & . & x_2^{n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{vmatrix}.$$

Para demostrar la fórmula (3) aplicamos la inducción sobre n. Considerando, que Δ_m, $m < n$, se calcula por medio de la fórmula (3), y apoyándonos en la propiedad D7, restamos de cada i-ésima fila del determinante Δ_n la $(i-1)$-ésima fila, multiplicada por x_1:

$$\Delta_n = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 0 & x_2 - x_1 & \ldots & x_n - x_1 \\ 0 & x_2^2 - x_2x_1 & \ldots & x_n^{n-1} - x_n^{n-2}x_1 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & x_2^{n-1} - x_2^{n-2}x_1 & \ldots & x_n^{n-1} - x_n^{n-2}x_1 \end{vmatrix}.$$

Surge la idea de desarrollar ahora a Δ_n por la primera columna, y al determinante de orden $n-1$ que se obtenga, sacar de la j-ésima columna ($j = 1, 2, \ldots, n-1$) fuera del signo del determinante, el multiplicador común $x_{j+1} - x_1$ (propiedad $D1'$ para las columnas). Llegamos a la expresión

$$\Delta_n = (x_n - x_1)(x_{n-1} - x_1) \ldots (x_2 - x_1) \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_2 & x_3 & \ldots & x_n \\ \cdot & \cdot & \cdot & \cdot \\ x_2^{n-2} & x_3^{n-2} & \ldots & x_n^{n-2} \end{vmatrix} =$$

$$= (x_n - x_1)(x_{n-1} - x_1) \ldots (x_2 - x_1) \cdot \Delta(x_2, x_3, \ldots, x_n),$$

que coincide con (3), por cuanto, por presupuesto de la inducción $\Delta(x_2, \ldots, x) = \prod_{2 \leqslant i < j \leqslant n} (x_j - x_i)$.

EJEMPLO 2. La matriz $A = (a_{ij})$ del tipo

$$A = \begin{vmatrix} 0 & a_{12} & a_{13} & a_{1n} \\ -a_{12} & 0 & a_{23} & a_{2n} \\ -a_{13} & -a_{23} & 0 & a_{3n} \\ \cdot & \cdot & \cdot & \cdot \\ -a_{1n} & -a_{2n} & -a_{3n} & 0 \end{vmatrix}$$

se denomina *antisimétrica* (de su determinante también se dice que es antisimétrico). En otras palabras, ${}^tA = -A$. Teniendo en cuenta el teorema 3, tenemos

$$\det A = \det {}^tA = \det(-A) = (-1)^n \det A,$$

de donde $[1 + (-1)^{n-1}] \det A = 0$. Para n impar obtenemos $\det A = 0$, o sea, *el determinante de cualquier matriz antisimétrica de orden impar, es nulo.*

4. Determinantes de matrices especiales. Cuanto más ceros hay entre los elementos de la matriz A, «cuanto mejor» ellos se encuentren

dispuestos, tanto más fácil resulta calcular el det A. Esta idea intuitiva encuentra en algunos casos una expresión cuantitativa exacta. Por ejemplo, sabemos (véase el punto 2 del § 1), que el determinante de una matriz triangular (superior o inferior) es igual al producto de los elementos que se encuentran en la diagonal principal. Otro caso particular importante contiene el

TEOREMA 4. *Para el determinante D, de orden $n + m$, en el que, en las intersecciones de las primeras n columnas con las últimas m filas, sólo se encuentran ceros, tiene lugar la fórmula*

$$\begin{vmatrix} a_{11} & a_{1n} & a_{1,n+1} & \dots & a_{1,n+m} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{nn} & a_{n,n+1} & \dots & a_{n,n+m} \\ 0 & 0 & b_{11} & \dots & b_{1m} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & b_{m1} & \dots & b_{mm} \end{vmatrix} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \cdot & \cdot & \cdot \\ a_{n1} & \dots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & \dots & b_{1m} \\ \cdot & \cdot & \cdot \\ b_{m1} & \dots & b_{mm} \end{vmatrix}$$

(el determinante del primer miembro de esta igualdad se llama *cuasitriangular*, o *determinante con un ángulo de ceros*).

DEMOSTRACION. Fijemos en principio $n(n + m)$ elementos a_{ij} y consideremos al determinante D como una función de los elementos b_{kl}, que conforman la matriz cuadrada B de orden m. La función obtenida se puede considerar como una función de la matriz $B: D = \mathscr{D}(B)$.

Es claro, que la multilinealidad y la antisimetría del determinante D respecto a las últimas m filas, es equivalente a las mismas propiedades de $\mathscr{D}(B)$ en relación a las filas de la matriz B. Quiere decir, que es correcto aplicar a $\mathscr{D}(B)$ el teorema 2 del § 1, de acuerdo al que $\mathscr{D}(B) = \mathscr{D}(E)\cdot\det B$. Por definición de la función $\mathscr{D}$ tenemos

$$\mathscr{D}(E) = \begin{vmatrix} a_{11} & \dots & a_{1n} & a_{1,n+1} & \dots & b_{1,n+m} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \dots & a_{nn} & a_{n,n+1} & \dots & a_{n,n+m} \\ 0 & \dots & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & 0 & 1 & \dots & 1 \end{vmatrix}$$

Desarrollemos a $\mathscr{D}(E)$ por la última fila (véase la fórmula (2)), luego por la penúltima, etc. Repitiendo esta operación m veces, nos convencemos de que $\mathscr{D}(E) = \det A$, donde

$$A = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \cdot & \cdot & \cdot \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Definitivamente obtenemos: $D = \mathscr{D}(B) = \det A \cdot \det B$. ∎

Con las nuevas designaciones, la fórmula del teorema 4 adopta una forma más compacta

$$\det \begin{Vmatrix} A & C \\ 0 & B \end{Vmatrix} = \det A \cdot \det B. \qquad (4)$$

Aquí, A y B son matrices cuadradas, y la matriz nula 0 y la matriz C son rectangulares. Apoyándonos en los teoremas 3 y 4 o en los razonamientos utilizados en el transcurso de la demostración del teorema 4, sin trabajo establecemos que,

$$\det \begin{Vmatrix} A & 0 \\ C & B \end{Vmatrix} = \det A \cdot \det B. \quad ■$$

A veces, prueban de escribir exactamente la misma expresión para el determinante del $\begin{Vmatrix} B & A \\ C & 0 \end{Vmatrix}$, aunque inmediatamente se sugiere un contraejemplo sencillísimo $\begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix} = -1$. Toda la cuestión radica en el signo. La respuesta correcta se obtiene mediante permutaciones de filas o de columnas, que llevan la matriz $\begin{Vmatrix} C & A \\ B & 0 \end{Vmatrix}$ a la forma $\begin{Vmatrix} C & 0 \\ B & A \end{Vmatrix}$ o $\begin{Vmatrix} A & C \\ 0 & B \end{Vmatrix}$.

Razonamientos más sencillos, se basan en el mismo teorema 2 del § 1, la cual hemos utilizado repetidamente. Efectivamente,

$$\det \begin{Vmatrix} C & A \\ B & 0 \end{Vmatrix} = \det \begin{Vmatrix} C & A \\ E & 0 \end{Vmatrix} \cdot \det B.$$

Luego, por la fórmula (1), aplicada m veces, hallamos

$$\det \begin{Vmatrix} C & A \\ E & 0 \end{Vmatrix} = \begin{vmatrix} \star & & a_{11} & \dots & a_{1n} \\ & & a_{n1} & \dots & a_{nn} \\ 1 & \dots & 0 & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & 1 & 0 & \dots & 0 \end{vmatrix} =$$

$$= (-1)^{(n+2)+(n+4)+\dots+(n+2m)} \det A = (-1)^{nm} \det A.$$

Definitivamente, llegamos a la conclusión que si A, B son matrices cuadradas de orden n y m respectivamente, entonces,

$$\det \begin{Vmatrix} C & A \\ B & 0 \end{Vmatrix} = (-1)^{nm} \det A \cdot \det B. \qquad (5)$$

Las fórmula (4) y (5) engloban al teorema general de Laplace sobre el desarrollo de determinantes. Este teorema, sin embargo, se utiliza relativamente poco, y no nos detendremos en él. Y no nos apuramos con la deducción del llamado teorema del desarrollo completo de un determinante (véase el cap. 4, § 3), que presta poco provecho desde el punto de vista del cálculo.

Una afirmación muy importante, acerca de los determinantes de matrices, contiene el siguiente

TEOREMA 5. *Sean A y B, matrices cuadradas de orden n. Entonces*

$$\det AB = \det A \cdot \det B.$$

DEMOSTRACION. De acuerdo con las fórmulas (7) y (9) del § 3 del cap. 2, que expresan los coeficientes c_{ij} de la matriz $(c_{ij}) = AB = (a_{ij})(b_{ij})$ por medio de los coeficientes de las matrices A y B, la i-ésima fila $(AB)_i$ se escribe de la forma

$$(AB)_i = (A_i B^{(1)},\ A_i B^{(2)},\ \ldots,\ A_i B^{(n)});$$

$$A_i B^{(j)} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Fijamos la matriz B y para cualquier matriz A hacemos

$$\mathscr{D}(A) = \det AB.$$

Demostremos, que la función $\mathscr{D}$ cumple las condiciones (i), (ii) del teorema 2 del § 1. Efectivamente, sabemos que el det AB: es una función lineal de los elementos de la i-ésima fila $(AB)_i$:

$$\det(AB) = \lambda_1 A_i B^{(1)} + \lambda_2 A_i B^{(2)} + \ldots + \lambda_n A_i B^{(n)}.$$

Por eso,

$$\mathscr{D}(A) = \sum_{j=1}^{n} \lambda_j \sum_{k=1}^{n} a_{ik} b_{kj} = \sum_{k=1}^{n} a_{ik} \sum_{j=1}^{n} \lambda_j b_{kj} = \sum_{k=1}^{n} \mu_k a_{ik},$$

donde $\mu_k = \sum_{j=1}^{n} \lambda_j b_{kj}$, es un escalar, independiente de los elementos de la i-ésima fila A_i de la matriz A.

Observamos, que $\mathscr{D}(A)$ es linealmente dependiente de los elementos de la i-ésima fila de la matriz A.

Luego, intercambiamos de lugar a A_s y A_t. Puesto que las s-ésima y t-ésima filas de la matriz AB tienen la forma

$$(A_s B^{(1)},\ \ldots,\ A_s B^{(n)}),$$
$$(A_t B^{(1)},\ \ldots,\ A_t B^{(n)}),$$

entonces, en este caso, ellas también se intercambian de lugar y, en consecuencia, por el teorema 1:

$$\mathscr{D}(\ldots, A_s, \ldots, A_t, \ldots) = \mathscr{D}(A) = \det AB =$$
$$= \det[\ldots, (AB)_s, \ldots, (AB)_t, \ldots] =$$
$$= -\det[\ldots (AB)_t, \ldots, (AB)_s, \ldots] =$$
$$= -\mathscr{D}(\ldots, A_t, \ldots, A_s, \ldots).$$

De este modo, se cumplen ambas condiciones del teorema 2 del § 1, de acuerdo al cual $\mathscr{D}(A) = \mathscr{D}(E) \cdot \det A$. Pero, por definición, $\mathscr{D}(E) = \det EB = \det B$. De donde se deduce la fórmula buscada. ∎

5. Sobre la construcción de la teoría de determinantes. Los teoremas 1 y 2 del § 1, dan, en esencia, una descripción axiomática de la función det, aunque comenzamos con su pura expresión constructiva.

Un camino más para la construcción de la teoría de los determinantes indica el teorema 2. Precisamente, sea que tenemos una función $\mathscr{D}: M_n(R) \to R$, poseedora de las siguientes propiedades:

(i) $\mathscr{D}(AB) = \mathscr{D}(A)\cdot\mathscr{D}(B)$, *para cualesquiera matrices* $A, B \in M_n(R)$;

(ii) $\mathscr{D}(F_{s,t}) = -1$ *para cada matriz elemental* $F_{s,t}$ (véase el punto 4 del § 4 del cap. 2);

(iii) $\mathscr{D}(A) = \lambda$, *para cada matriz triangular superior del tipo*

$$A = \begin{Vmatrix} \lambda & & & \\ & 1 & & * \\ & & \ddots & \\ 0 & & & 1 \end{Vmatrix}, \quad \lambda \in R.$$

Se afirma, que $\mathscr{D} = \det$. Efectivamente, aprovechándose de la propiedad (i) empleándola en la matriz

$$B = F_{1,s}\begin{Vmatrix} \lambda & & & \\ & 1 & & * \\ & & \ddots & \\ 0 & & & 1 \end{Vmatrix} F_{1,s} = \begin{Vmatrix} 1 & & & & * \\ & \ddots & & & \\ & & \lambda & & \\ & & & \ddots & \\ 0 & & & & 1 \end{Vmatrix},$$

obtenemos $\mathscr{D}(B) = (-1)\cdot\lambda\cdot(-1) = \lambda$. Esto significa, que $\mathscr{D}(F_s(\lambda)) = \lambda$ para la matriz elemental $F_s(\lambda)$. De acuerdo con (iii), $\mathscr{D}(F_{s,t}(\lambda)) = 1$ para la matriz elemental $F_{s,t}(\lambda)$ con $s < t$. Como

$$F_{s,t}\cdot F_{s,t}(\lambda)\cdot F_{s,t} = F_{t,s}(\lambda),$$

entonces, y $\mathscr{D}(F_{t,s}(\lambda)) = 1$, y por eso, $\mathscr{D}(F_{s,t}(\lambda)) = 1$, para cualesquiera índices $s \neq t$.

Así $\mathscr{D}(F_{s,t}) = -1$, $\mathscr{D}(F_{s,t}(\lambda)) = 1$ y $\mathscr{D}(F_s(\lambda)) = \lambda$. Por cuanto, cualquier matriz $A \in M_n(R)$ se escribe de forma $A = P\begin{Vmatrix} E_r & 0 \\ 0 & 0 \end{Vmatrix}Q$, $r \leqslant n$, donde P y Q son productos de matrices elementales (véanse los razonamientos anteriores al teorema 5 del § 4 del cap. 2), la propiedad (i) permite efectivamente calcular $\mathscr{D}$ (A).

Sea que la matriz A' se obtuvo multiplicando la s-ésima fila A_s de la matriz A por λ, o sumando a A_s la fila A_t con el número t. Entonces, como se hizo notar en el cap. 2, $A' = F_s(\lambda)\cdot A$, o también $A' = F_{s,t}(1)\cdot A$. En el primer caso, tenemos $\mathscr{D}(A') = \lambda\cdot\mathscr{D}(A)$, y en el segundo, $\mathscr{D}(A') = \mathscr{D}(A)$. Dicho de otro modo, $\mathscr{D}(A)$ es función multilineal de las filas de la matriz A.

Si, además, A' se obtuvo de A por una permutación de filas con números s y t, entonces, $A' = F_{s,t}A$, de donde $\mathscr{D}(A') = \mathscr{D}(F_{s,t})\cdot\mathscr{D}(A) = -\mathscr{D}(A)$. O sea, $\mathscr{D}(A)$ es una función antisimétrica de las filas de la matriz A.

Finalmente, $\mathscr{D}(E) = \mathscr{D}(F_s(1)) = 1$.

Vemos, que la función $\mathscr{D}$ posee las tres propiedades básicas $D1 - D3$ de los determinantes. Así pues, por el teorema 2 del § 1 $\mathscr{D}(A) = \det A$.

Se le propone al lector plantear y fundamentar variantes propias de descripción axiomática de la función det.

EJERCICIOS

1. Los números enteros $1798 = 31\cdot 58$, $2139 = 31\cdot 69$, $3255 = 31\cdot 105$, $4867 = 31\cdot 157$, son divisibles por 31. Sin ningún cálculo, mostrar que el determinante de cuarto orden

$$\begin{Vmatrix} 1 & 7 & 9 & 8 \\ 2 & 1 & 3 & 9 \\ 3 & 2 & 5 & 5 \\ 4 & 8 & 6 & 7 \end{Vmatrix}$$

también es divisible por 31.

2. Mostrar, que cualquier determinante antisimétrico de cuarto orden $|a_{ij}|$ con $a_{ij} \in \mathbb{Z}$, es cuadrado de un número entero. (*Observación*. Esto es cierto para cualquier determinante antisimétrico).

3. Demostrar la relación $\det AB = \det A\cdot\det B$ (teorema 5), mediante la reducción empleando transformaciones elementales del tipo (II) sobre las filas, de la matriz auxiliar $C = \begin{Vmatrix} E & B \\ -A & 0 \end{Vmatrix}$ de dimensiones $2n \times 2n$, a la forma $C' = \begin{Vmatrix} E & B \\ 0 & AB \end{Vmatrix}$. (*Indicación*. Aprovechar la igualdad $\det C = \det C'$ y las relaciones (4), (5).

4. Mostrar, que ${}^t(AB)\,{}^tB\,{}^tA$, para cualesquiera matrices rectangulares A, B, de dimensiones $m \times r$ y $r \times n$.

5. Mostrar, que $\det B^{-1}AB = \det A$, para cualquier matriz cuadrada $A \in M_n(\mathbb{R})$ y cualquier matriz invertible $B \in M_n(\mathbb{R})$.

6. Sea

$$C_n(\lambda_1, \ldots, \lambda_n) = \begin{Vmatrix} \lambda_1 & 0 & 0 & \ldots & 0 & 0 & 0 \\ -1 & \lambda_2 & 1 & \ldots & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & \lambda_{n-2} & 1 & 0 \\ 0 & 0 & 0 & \ldots & -1 & \lambda_{n-1} & 1 \\ 0 & 0 & 0 & \ldots & 0 & -1 & \lambda_n \end{Vmatrix}.$$

Mostrar, que $\det C_n = \lambda_n \det C_{n-1} + \det C_{n-2}$. Para $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 1$, hallar el valor numérico del $\det C_n$. (*Indicación*. Recordar el ejemplo 3 del punto 3 del § 3 del cap. 2, y prestar atención al hecho, de que $\det C_n(1, \ldots, 1) = (-1)^{n-1} \det C_n(-1, \ldots, -1)$).

7. Mostrar, que el determinante $n \times n$ de la matriz

$$A_n = \begin{Vmatrix} 2 & -1 & 0 & 0 & \ldots & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & \ldots & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \ldots & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & \ldots & 0 & -1 & 2 \end{Vmatrix}$$

es igual a $n+1$.

§ 3. APLICACION DE LOS DETERMINANTES

1. Criterio de no degeneración de una matriz. En el § 3 del cap. 2, la matriz cuadrada A se llamó no degenerada, si existe una matriz inversa a ella A^{-1}. Aplicando el teorema 5 del § 2 a la relación $AA^{-1} = A^{-1}A = E$, obtenemos, que $\det A \cdot \det A^{-1} = 1$. Así pues, el *determinante de una matriz no degenerada es distinto de cero y*

$$\det A^{-1} = (\det A)^{-1}.$$

Juntamente con la matriz A examinemos su matriz *adjunta* (o *recíproca*)

$$A^{\vee} = \begin{Vmatrix} A_{11} & \dots & A_{n1} \\ \dots & \dots & \dots \\ A_{1n} & \dots & A_{nn} \end{Vmatrix}.$$

A fin de obtener $A^{\vee}$, hay que colocar en el lugar de cada elemento a_{ij} de la matriz A, a su complemento algebraico A_{ij} ($i, j = 1, \dots, n$), y luego proceder a la trasposición de la matriz.

TEOREMA 1. *La matriz $A \in M_n(\mathbb{R})$ es no degenerada (invertible) si, y sólo si,* $\det A \neq 0$. *Si* $\det A \neq 0$, *entonces* $A^{-1} = (\det A)^{-1} A^{\vee}$, *o, en escritura más detallada:*

$$\begin{Vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{Vmatrix}^{-1} = \begin{Vmatrix} \dfrac{A_{11}}{\det A} & \dots & \dfrac{A_{n1}}{\det A} \\ \dots & \dots & \dots \\ \dfrac{A_{1n}}{\det A} & \dots & \dfrac{A_{nn}}{\det A} \end{Vmatrix}.$$

A la demostración del teorema le anticipamos un lema.

TEOREMA 1. *Sea $A \in M_n(\mathbb{R})$. Tienen lugar las relaciones*

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \dots + a_{in}A_{jn} = \delta_{ij} \det A, \tag{1}$$
$$a_{1i}A_{1j} + a_{2i}A_{2j} + \dots + a_{ni}A_{nj} = \delta_{ij} \det A, \tag{2}$$

donde δ_{ij} es el símbolo de Kronecker (cuando $i \neq j$ se habla sobre el desarrollo del determinante por una fila ajena, o por una columna ajena, respectivamente).

DEMOSTRACION. Cuando $i = j$, la afirmación del lema coincide con los teoremas 1 y 1' del § 2. Por eso, queda por examinar el caso $i \neq j$, cuando $\delta_{ij} = 0$. Con este fin introducimos la matriz

$$A' = [A_1, \dots, A_j, \dots, A_i, \dots, A_n] = \begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix}$$

que se obtiene de $A = [\ldots, A_i, \ldots, A_j, \ldots]$ cambiando la j-ésima fila por la i-ésima (la i-ésima queda en su lugar.) Como cualquier otra matriz cuadrada con dos filas iguales, el det $A' = 0$. Por otro lado, el complemento algebraico A'_{jk} ($k = 1, \ldots, n$) se forma tachando la j-ésima fila $A'_j = A_i$ y de la k-ésima columna del determinante, así que $A'_{jk} = A_{jk}$. El desarrollo formal del determinante de la matriz $A' = (a'_{st})$ por la j-ésima fila nos da la relación

$$0 = \det A' = \sum_{k=1}^{n} a'_{jk}A'_{jk} = \sum_{k=1}^{n} a_{ik}A_{jk},$$

coincidente con la expresión (1) en la formulación del lema. La segunda relación se obtiene de reflexiones análogas, referidas a las columnas. $\blacksquare$

Volviendo a la demostración del teorema, sencillamente observamos, que el primer miembro de la relación (1) no es otra cosa, que el elemento c_{ij} de la matriz $C = AA^\vee$:

$$\left\| \begin{matrix} c_{11} & \ldots & c_{1n} \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ c_{n1} & \ldots & c_{nn} \end{matrix} \right\| = \left\| \begin{matrix} a_{11} & \ldots & a_{1n} \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ a_{n1} & \ldots & a_{nn} \end{matrix} \right\| \left\| \begin{matrix} A_{11} & \ldots & A_{n1} \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ A_{1n} & \ldots & A_{nn} \end{matrix} \right\|.$$

De acuerdo a la relación (1) $(c_{ij}) = (\delta_{ij} \det A) = (\det A)\, E$. De este modo,

$$AA^\vee = (\det A)\, E,$$

de donde, para $\det A \neq 0$ obtenemos

$$(\det A)^{-1}\,(AA^\vee) = A\,(\det A)^{-1}A^\vee = E.$$

El primer miembro de la relación (2) es expresión del elemento c'_{ji} de la matriz $C' = A^\vee A$. Puesto que los segundos miembros en (1) y (2) coinciden, entonces, en el caso en que $\det A \neq 0$ llegamos a las relaciones

$$A\,(\det A)^{-1}A^\vee = (\det A)^{-1}A^\vee A = E,$$

que significa que $A^{-1} = (\det A)^{-1}A^\vee$. $\blacksquare$

COROLARIO 1. *Un determinante es nulo si, y sólo si, sus filas (o columnas) son linealmente dependientes.*

Este criterio, nos es parcialmente conocido (véase el final del punto 3 del § 2) y pudo haber sido demostrado mucho antes, pero no hubo necesidad de él. El razonamiento: por el teorema 1 la igualdad $\det A = 0$ es equivalente a la degeneración de la matriz A, y el degeneramiento, por el teorema 4 del § 3 del cap. 2, es equivalente a la condición de que $\operatorname{rank} A < n$ ($n \times n$ son las dimensiones de la matriz A), que caracteriza, en virtud del teorema 1 del § 2 del cap. 2, a la matriz con filas (columnas) linealmente dependientes. $\blacksquare$

El teorema 1 tiene más bien significado teórico. Desde el punto de vista del cálculo, en especial para grandes dimensiones de las

matrices, en la búsqueda de la matriz A^{-1} es más cómodo utilizar el método (P, Q)-reducción, descripto en el corolario del teorema 5 del § 4 del cap. 2.

Deduzcamos ahora fórmulas para resolver sistemas de n ecuaciones lineales con n incógnitas, debido a las cuales, en particular, fue inicialmente desarrollada la teoría de determinantes.

COROLARIO 2 (Regla de Cramer). *Si el sistema lineal*

$$\begin{aligned} a_{11}x_1 + \ldots + a_{1n}x_n &= b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + \ldots + a_{nn}x_n &= b_n \end{aligned}$$

tiene determinante distinto de cero (o sea, $\det(a_{ij}) \neq 0$*), entonces, su solución única es dada por la fórmula*

$$x_k^0 = \frac{\begin{vmatrix} a_{11} & \ldots & b_1 & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & b_n & \ldots & a_{nn} \end{vmatrix}}{\begin{vmatrix} a_{11} & \ldots & a_{1k} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nk} & \ldots & a_{nn} \end{vmatrix}}, \quad k = 1, 2, \ldots, n$$

(el numerador D_k *se obtiene cambiando a la k-ésima columna de* $D = \det(a_{ij})$*, por la columna de términos independientes).*

DEMOSTRACION. Por el teorema 1, la matriz $A = (a_{ij})$ es invertible. Por eso, escribiendo nuestro sistema de forma $AX = B$, como en el § 4 del cap. 2, obtenemos

$$X = A^{-1}B = \frac{(A_{ji})\,B}{\det A},$$

de donde

$$x_k^0 = \frac{\sum_j A_{jk}b_j}{\det A}.$$

Precisamente, esta expresión obtenemos en el numerador, desarrollando el determinante D_k, por la k-ésima columna (véase (2)). ■

Cumpliendo todas las transformaciones en orden contrario, se muestra, que el conjunto $(D_1/\det A, \ldots, D_n/\det A)$, efectivamente, es solución de nuestro sistema. ■

Observemos, que las fórmulas (3), (9) del § 4 del cap. 1 coinciden, justamente, con las reglas de Cramer para $n = 2$ y 3, respectivamente. Cómodas para n pequeñas, las reglas de Cramer cumplen, en general, una función puramente teórica. Por ejemplo, empleándolas para el sistema lineal del ejemplo 2 en el punto 4 del § 3 del cap. 1, da (teniendo en cuenta la igualdad $\det A = 1$) la

expresión para los números de Fibonacci

$$f_n = \begin{Vmatrix} 1 & 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 1 & 0 & \dots & 0 & 0 & 1 \\ -1 & -1 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & -1 & 1 & 0 \\ 0 & 0 & 0 & \dots & -1 & -1 & 0 \end{Vmatrix}.$$

Se comprende, que esta fórmula está lejos de la clara expresión de f_n hallada al final del § 3 del cap. 2.

2. Cálculo del rango de una matriz. En los §§ 2 y 4 del cap. 2 está contenido todo lo necesario para describir un cúmulo de resoluciones del sistema rectangular general de ecuaciones lineales. El papel principal en esta descripción, le corresponde al concepto de rango de una matriz. Nos queda sólo traducirlo a la lengua de la teoría de determinantes, para tener a nuestra disposición otro método más de cálculo del rango y un medio cómodo para expresar el hecho de la independencia lineal de un sistema de vectores del espacio lineal aritmético $\mathfrak{R}^n$.

De suerte que, sea

$$A = \begin{Vmatrix} a_{11} & \dots & a_{1r} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} & \dots & a_{rn} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a_{mr} & \dots & a_{mn} \end{Vmatrix}$$

una matriz rectangular cualquiera, de dimensiones $m \times n$, con coeficientes $a_{ij} \in \mathfrak{R}$. Bajo el nombre de menor de k-ésimo orden de la matriz A, como de costumbre, se entiende al determinante de la matriz de los elementos, que se encuentran en A, en las intersecciones de las k columnas y k filas distintas, señaladas: $k \leqslant \min(n, m)$.

Sea que el rango de la matriz A es igual a r. De acuerdo con el teorema 1 del § 2 del cap. 2, esto significa, que r es el número máximo de filas linealmente independientes, y el número máximo de columnas linealmente independientes de la matriz A. Volviendo al teorema 5 del § 4 del cap. 2 y su corolario, notamos que

$$A = B \begin{Vmatrix} E_r & 0 \\ 0 & 0 \end{Vmatrix} C,$$

donde B y C son matrices no degeneradas, de dimensiones $m \times m$ y $n \times n$, respectivamente, escritas en forma de producto de matrices elementales. Como en la matriz $\begin{Vmatrix} E_r & 0 \\ 0 & 0 \end{Vmatrix}$ se tiene un menor $M =$

$= |E_r| = 1$, distinto de cero, de orden r, no hay menores no nulos de orden $> r$, y como esta propiedad se conserva con transformaciones elementales de las filas y de las columnas, entonces, llegamos a la siguiente afirmación.

TEOREMA 2. *El rango de cualquier matriz A, $m \times n$, es igual al orden mayor de sus menores distintos de cero.* ∎

Cualquier menor distinto de cero del orden *máximo* de la matriz A, se llama *menor básico*. Las columnas (correspondientemente, las filas) de la matriz A, que intersecan al menor básico dado, se llaman, de acuerdo con la terminología del cap. 2, columnas básicas (correspondientemente, filas básicas). Como de costumbre, interpretando las filas y columnas de la $m \times n$-matriz A, como vectores de los espacios $\mathcal{R}^n$ y $\mathcal{R}^m$, respectivamente, y también utilizando las propiedades básicas de los sistemas de vectores linealmente independientes (su complementación hasta la base; véase el ejercicio 5 del § 1 del cap. 2), es fácil comprender, que la búsqueda de por lo menos un menor básico se puede simplificar sensiblemente, si se examinan consecuentemente los llamados *menores orlados*. Precisamente, si es hallado un menor M de k-ésimo orden de la matriz A, distinto de cero, entonces, el paso siguiente consiste en la verificación de sólo aquellos menores de $(k + 1)$-ésimo orden, de los cuales M se obtiene eliminando una fila y una columna. Si, esos menores, que orlan a M, son nulos, entonces, el rango de rank $A = k$. (¿Porqué? Esto significaría, por el teorema 2, que cualquier columna de la matriz A se expresa linealmente por medio de las k columnas elegidas.) En caso contrario, se debe pasar a los menores que orlan algún menor no nulo, de orden $k + 1$.

El método de los menores orlados es suficientemente práctico, especialmente, cuando deseamos saber no sólo el rango, sino también las columnas o filas de la matriz A, que componen el sistema maximal linealmente independiente. Al emplear transformaciones elementales esta información, por supuesto, se pierde.

EJERCICIOS

1. Mostrar, que se cumplen las siguientes relaciones:

$$(AB)^{\vee} = B^{\vee} A^{\vee}; \quad ({}^tA)^{\vee} = {}^t(A^{\vee}); \quad (\lambda A)^{\vee} = \lambda^{n-1} A^{\vee}; \quad (A^{\vee})^{\vee} = (\det A)^{n-2} A.$$

2. Expresar el rank $A^{\vee}$, por medio del rank A.

3. Demostrar, que el sistema cuadrado de ecuaciones lineales homogéneas, tiene solución no trivial si, y sólo si, el determinante del sistema es nulo.

4. Basándose en los resultados del punto 1 del § 4 del cap. 2 y en el corolario 2 del teorema 1, mostrar, que el sistema fundamental de soluciones, del sistema homogéneo

$$\begin{gathered} a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ \ldots\ldots\ldots\ldots \\ a_{n-1\,1}x_1 + \ldots + a_{n-1,\,n}x_n = 0 \end{gathered}$$

de rango $r = n - 1$, se compone de un vector-columna

$$X^0 = [D_1, -D_2, D_3, \ldots, (-1)^{n-1} D_n],$$

donde D_i es el determinante de la matriz que se obtiene de $A = (a_{ij})$ eliminando su i-ésima columna. Cualquier solución del sistema tiene la forma $X = \lambda X^0$.

5. Sean, $A = (a_{ij}) \in M_n(K)$, y $(n-1) \mid a_{ij} \mid < \mid a_{ii} \mid$ para todos los $i \neq j$. Demostrar, que det $A \neq 0$. (*Indicación*. Suponiendo lo contrario, utilizar el criterio formulado en el ejercicio 3. Precisamente, si $[x_1^0, \ldots, x_n^0]$ es solución no trivial del sistema lineal $AX = 0$ y x_k^0 es su componente, que tiene el módulo máximo, entonces, de la k-ésima ecuación $a_{kk}x_k^0 + \sum_{j \neq k} + a_{kj}x_j^0 = 0$,

sigue la estimación $(n-1)|a_{kk}|\,|x_k^0| = (n-1)\left|\sum_{j \neq k} a_{kj}x_j^0\right| < (n-1)|a_{kk}|\,|x_k^0|$,

que brinda la contradicción necesaria).

6. Demostrar la siguiente afirmación. Sean $A = (a_{ij})$, $B = (b_{kl})$, matrices de dimensiones $n \times m$ y $m \times n$, respectivamente, y sea $C = AB$. Entonces

$$\det C = \sum_{1 \leqslant j_1 < \ldots < j_n \leqslant m} \begin{vmatrix} a_{1j_1} & a_{2j_1} & \ldots & a_{nj_1} \\ a_{1j_2} & a_{2j_2} & \ldots & a_{nj_2} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1j_n} & a_{2j} & \ldots & a_{nj_n} \end{vmatrix} \begin{vmatrix} b_{j_1 1} & b_{j_1 2} & \ldots & b_{j_1 n} \\ b_{j_2 1} & b_{j_2 3} & \ldots & b_{j_2 n} \\ \cdot & \cdot & \cdot & \cdot \\ b_{j_n 1} & b_{j_n 2} & \ldots & b_{j_n n} \end{vmatrix}$$

En el segundo miembro, la suma se efectúa para todas las $\binom{m}{n}$ combinaciones posibles de n elementos $\{j_1, j_2, \ldots, j_n\}$ tomados de $1, 2, \ldots, m$. En particular, det C = det A · det B para $m = n$ y det $C = 0$, para $n > m$. (*Indicación*. Como $C = (c_{ij})$, $c_{ij} = \sum a_{ik}b_{kj}$, entonces, el uso repetido de la regla de desarrollo de un determinante por una fila (teorema 1' del § 2 del cap. 3), da

$$\det C = \sum_{k_1, \ldots, k_n = 1}^{n} \begin{vmatrix} a_{1k_1} & a_{1k_2} & \ldots & a_{1k_n} \\ a_{2k_1} & a_{2k_2} & \ldots & a_{2k_n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{nk_1} & a_{nk_2} & \ldots & a_{nk_n} \end{vmatrix} b_{k_1 1}\, b_{k_2 2} \ldots a_{nk_n},$$

donde la suma se realiza para todos los pares de $k_1, \ldots, k_n$ distintos. Cuando $m < n$, no existen tales índices, y, en consecuencia, det $C = 0$. Si $m \geqslant n$, entonces, $k_1, \ldots, k_n$, es una muestra de los elementos $\{j_1, \ldots, j_n\}$, tomados en algún orden, de $1, 2, \ldots, m$. Se deben juntar todos los miembros, en correspondencia con la combinación dada $\{j_1, \ldots, j_n\}$, y con la ayuda del teorema sobre el desarrollo completo de un determinante, obtener

$$\sum \begin{vmatrix} a_1k_1 & \ldots & a_nk_1 \\ \cdot & \cdot & \cdot \\ a_1k_n & \ldots & a_nk_n \end{vmatrix} b_{k_1 1} \ldots b_{k_n n} =$$

$$= \begin{vmatrix} a_{1j_1} & \ldots & a_{nj_1} \\ \cdot & \cdot & \cdot \\ a_{1j_n} & \ldots & a_{nj_n} \end{vmatrix} \sum_{\pi} \varepsilon_\pi b_{k_1 1} \ldots b_{k_n 1} =$$

$$=\begin{vmatrix} a_{1j_1} & \dots & a_{nj_1} \\ \cdot & \cdot & \cdot \\ a_{1j_n} & \dots & a_{nj_n} \end{vmatrix} \begin{vmatrix} b_{j_11} & \dots & b_{j_1n} \\ \cdot & \cdot & \cdot \\ b_{j_n1} & \dots & a_{j_nn} \end{vmatrix},$$

donde $\pi \doteq \begin{pmatrix} j_1 & \dots & j_n \\ k_1 & \dots & k_n \end{pmatrix}$.

7. Utilizando el ejercicio anterior, mostrar, que si A es una $m \times n$-matriz sobre $\mathfrak{K}$, $m \geqslant n$, entonces

$$\det {}^tAA = \sum_M M^2,$$

donde M recorre por todos los $\binom{m}{n}$ menores de orden n de la matriz A.

Capítulo 4

ESTRUCTURAS ALGEBRAICAS

(grupos, anillos, campos)

En los capítulos precedentes se acumuló suficiente material concreto, al que es necesario conceptualizar desde posiciones más generales. Con este fin, introducimos y estudiamos, por el momento en un nivel elemental, los conceptos fundamentales para todo el álgebra, de grupo, anillo y campo.

§ 1. CONJUNTOS CON OPERACIONES ALGEBRAICAS

1. Operaciones binarias. Sea X un conjunto cualquiera. Se llama *operación algebraica binaria* (o *ley de composición*) en X, la aplicación arbitraria (pero dada) τ: $X \times X \to X$ del cuadrado cartesiano $X^2 = X \times X$ en X. De este modo, a cada par ordenado (a, b) de los elementos $a, b \in X$, se pone en correspondencia de modo unívoco un tercer elemento determinado $\tau(a, b)$ perteneciente al mismo conjunto X. A veces, en lugar de $\tau(a, b)$ se escribe $a \tau b$, y más frecuentemente, la operación binaria en X se designa con algún símbolo especial: $*$, $\circ$, $\cdot$ y $+$. Seguimos nosotros el mismo camino, llamando $a \cdot b$ (o sencillamente ab, sin ningún signo entre a y b) *producto*, y $a + b$, *suma de los elementos* a, $b \in X$. Se comprende, que estos nombres, en la mayoría de los casos, son convencionales.

Hablando en general, en X se pueden dar muchas operaciones distintas. Deseando separar una de ellas, se emplean paréntesis $(X, *)$ y se dice, que la operación $*$ determina en X una *estructura algebraica* o que $(X, *)$ es un *sistema algebraico*. Así, por ejemplo, en el conjunto $\mathbb{Z}$ de los números enteros, además de las operaciones naturales $+$, $\cdot$ (suma y multiplicación), es fácil mostrar operaciones «derivadas», obtenidas con ayuda de $+(0 -)$y$\cdot$: $n \circ m = n + m - nm$, $n * m = -n - m$, etc. Obtenemos diferentes estructuras algebraicas $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, *)$.

Juntamente con las operaciones algebraicas binarias, no carecen de interés las mucho más generales n-arias operaciones (unarias cuando $n = 1$, ternarias cuando $n = 3$, etc.), al igual que sus combinaciones. Las estructuras algebraicas relacionadas con ellas, componen la teoría especial de álgebras universales. Todo esto lo mencionamos solamente para subrayar otra vez la importancia fundamental que tienen para las matemáticas, algo que parecería como partes propias de la teoría de álgebras universales, las estructuras algebraicas con operaciones binarias.

En el sentido de la construcción de distintas operaciones binarias en el conjunto X también, evidentemente, se abre un espacio ilimitado a la fantasía. Pero la tarea del estudio de estructuras

algebraicas arbitrarias es demasiado general para que represente algún valor real. Por esta causa, se efectúa con distintas limitaciones naturales.

2. Subgrupos y monoides. La operación binaria * en el conjunto X es *asociativa*, si $(a * b) * c = (a * (b * c)$ para todas, a, b c, $\in X$; se dice que es *conmutativa*, si $a * b = b * a$. Los mismos nombres se le otorgan a la correspondiente estructura algebraica $(X, *)$. Las exigencias de asociatividad y conmutatividad son independientes. De hecho, la operación * en $\mathbb{Z}$, dada por la regla $n * m = -n - m$, evidentemente, es conmutativa, pero $(1 * 2) * 3 = (-1-2) * 3 = -(1-2) - 3 = 0 \neq 4 = 1 * (2 * 3)$, así que la condición de asociatividad no se cumple. Luego, en el conjunto $M_n(\mathbb{R})$ de todas las matrices cuadradas de orden $n > 1$, está definida la operación de multiplicación, que es asociativa pero no conmutativa (véase el punto 2 del § 3 del cap. 2).

El elemento $e \in X$ se llama *unidad* (o *neutro*) en relación con la operación binaria considerada *, si $e * x = x * e = x$, para todas las $x \in X$. Si e' es otro elemento unidad, entonces, como se deduce de la definición, $e' = e' * e = e$. Así que, en la estructura algebraica $(X, *)$ no puede existir más de un elemento unidad.

El conjunto X, con una operación asociativa binaria dada en él, se llama *semigrupo*. Al semigrupo con elemento unidad (neutro) se acepta denominarlo *monoide* (o sencillamente, *semigrupo con unidad*).

Al igual que para cualquier grupo, la potencia del monoide $M = (M, *)$ se designa con el símbolo Card M o $|M|$. En el caso de un número finito de elementos contenidos en él, se habla de un monoide finito M de orden $|M|$.

Daremos algunos ejemplos de semigrupos y de monoides.

1) Sea Ω un conjunto arbitrario y $M(\Omega)$ el conjunto de todas sus transformaciones (aplicaciones de Ω en sí mismo). De las propiedades de los conjuntos y de las aplicaciones, señaladas en el § 5 del cap. 1, se deduce, que $M(\Omega)$ es un monoide. Se tiene en consideración, por supuesto, el trío $(M(\Omega), \circ, e_\Omega)$, donde $\circ$ es la composición natural de las aplicaciones, y el Ω es la aplicación idéntica.

Destaquemos el caso particular, cuando Ω es un conjunto finito de $|\Omega| = n$ elementos, designados sencillamente con los números naturales $1, 2, \ldots, n$. Cada transformación $f: \Omega \to \Omega$ se define por la sucesión ordenada señalada $f(1), f(2), \ldots, f(n)$, donde en calidad de imagen $f(i)$ puede estar cualquier elemento de Ω. No se excluye la coincidencia $f(i) = f(j)$ para $i \neq j$. Eligiendo todas las sucesiones posibles, obtenemos exactamente n^n transformaciones. Entonces, $|M(\Omega)| = \text{Card } M(\Omega) = n^n$. Sea, digamos, $n = 2$. Los elementos e, f, g, h del monoide $M(\{1, 2\})$ y sus productos pares, son dados en su totalidad por las dos tablas:

	1	2
e	1	2
f	2	1
g	1	1
h	2	2

·	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	g	g	g
h	h	h	h	h

Inmediatamente se aprecia, que $M(\{1, 2\})$ es un monoide no conmutativo.

2) Sea otra vez Ω un conjunto arbitrario, y $\mathcal{P}(\Omega)$ el conjunto de todos sus subconjuntos (véase el ejercicio 4 del § 5 del cap. 1). Como $(A \cap B) \cap C = A \cap (B \cap C)$ y $(A \cup B) \cup C = A \cup (B \cup C)$, entonces, en $\mathcal{P}(\Omega)$ se definen dos operaciones binarias naturales asociativas. Es evidente, que $\varnothing \cup A = A$ y $A \cap \Omega = A$. Tenemos dos monoides conmutativos $(\mathcal{P}(\Omega), \cup, \varnothing)$ y $(\mathcal{P}(\Omega), \cup, \Omega)$. Como se sabe, $|\mathcal{P}(\Omega)| = 2^n$, si $|\Omega| = n$.

3) $(M_n(\mathbb{R}), +, 0)$ es un monoide conmutativo con elemento neutro, una matriz nula, y $(M_n(\mathbb{R}), \cdot, E)$ es un monoide no conmutativo con elemento neutro, la matriz unidad E. Esto surge inmediatamente de las propiedades de la suma y de la multiplicación de matrices, las que hemos conocido en el cap. 2.

4) Sea $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$ un conjunto de números enteros divisibles por n. Es claro, que $(n\mathbb{Z}, +, 0)$ es un monoide conmutativo, y $(n\mathbb{Z}, \cdot)$ un subgrupo conmutativo sin unidad $(n > 1)$.

5) El conjunto $P_n(\mathbb{R})$ de matrices estocásticas de orden n (véase el ejercicio 8 del § 3 del cap. 2) es un monoide con una operación habitual de multiplicación de matrices.

El subconjunto S' del semigrupo S con la operación $*$, se llama *subsemigrupo*, si $x * y \in S'$ para todos los $x, y \in S'$. En este caso también se dice, que el *subconjunto* $S' \subset S$ es *cerrado respecto a la operación* $*$. Si $(M, *)$ es un monoide, y el subconjunto $M' \subset M$ no sólo es cerrado respecto a la operación $*$, sino que también contiene el elemento unidad, entonces M' se llama *submonoide* en M. Por ejemplo, $(n\mathbb{Z}, \cdot)$ es un subsemigrupo en $(\mathbb{Z}, \cdot)$, y $(n\mathbb{Z}, +, 0)$ un submonoide en $(\mathbb{Z}, +, 0)$. Todo submonoide del monoide $M(\Omega)$ se denomina *monoide de transformación* (del conjunto Ω).

3. Asociatividad generalizada; potencias. Sea $(X, \cdot)$ una estructura algebraica arbitraria con operación binaria $\cdot$, a la que, por sencillez, la omitiremos, escribiendo xy en lugar de $x \cdot y$. Sea, luego, $x_1, \ldots, x_n$, una sucesión ordenada de elementos de X. Sin cambiar el orden, de muchos modos podemos formar un producto de largo n. Sea l_n el número de tales modos:

$l_2 = 1: x_1x_2;$

$l_3 = 2: (x_1x_2)\,x_3,\ x_1\,(x_2x_3);$

$l_4 = 5: ((x_1x_2)\,x_3)\,x_4,\ (x_1\,(x_2x_3))\,x_4,\ x_1\,((x_2x_3)\,x_4),\ x_1\,(x_2\,(x_3x_4)),$

$(x_1x_2)\,(x_3x_4)$; etc.

Es evidente que, escogiendo todos los productos posibles $x_1, \ldots x_k$, $x_{k+1} \ldots x_n$ de largos k y $n-k$, $1 \leqslant k \leqslant n-1$, y luego uniéndolos mediante nuestra operación binaria en el orden dado, agotamos todas las l_n posibilidades. Es notable, que en los monoides (y subgrupos) la colocación de paréntesis resulta innecesaria.

TEOREMA 1. *Si una operación binaria en X es asociativa, entonces, el resultado de su aplicación consecutiva a n elementos del conjunto X, no depende de la colocación de paréntesis.*

DEMOSTRACION. Para $n = 1, 2$ no hay nada que demostrar. Para $n = 3$ la afirmación del teorema coincide con la ley de asociatividad.

Seguimos razonando por inducción sobre n. Supongamos que $n > 3$ y que para el número de elementos $< n$ la veracidad de la afirmación está establecida. Es necesario sólo demostrar que,

$$(x_1 \ldots x_k)(x_{k+1} \ldots x_n) = (x_1 \ldots x_l)(x_{l+1} \ldots x_n) \qquad (1)$$

para cualesquiera k, l, $1 \leqslant k$, $l \leqslant n - 1$. Transcribimos sólo los pares exteriores de paréntesis, por cuanto, por presupuesto de la inducción, la disposición de los paréntesis interiores no es esencial. En particular, $x_1x_2 \ldots x_k = (\ldots((x_1x_2)x_3) \ldots x_{k-1})x_k$ es un producto, llamado *normalizado a la izquierda*. Distinguimos dos casos:

a) $k = n - 1$. Entonces $(x_1 \ldots x_{n-1})x_n = (\ldots(x_1x_2) \ldots$ $\ldots x_{n-1})x_n$ es un producto normalizado a la izquierda.

b) $k < n - 1$. En virtud de la asociatividad tenemos

$$\begin{aligned}(x_1 \ldots x_k)(x_{k+1} \ldots x_n) = (x_1 \ldots x_k)((x_{k+1} \ldots \\ \ldots x_{n-1})x_n) = ((x_1 \ldots x_k)(x_{k+1} \ldots x_{n-1}))x_n = \\ = (\ldots((\ldots(x_1x_2) \ldots x_k)x_{k+1}) \ldots x_{n-1})x_n\end{aligned}$$

o sea, de nuevo un producto normalizado a la izquierda. A la misma forma se lleva el segundo miembro de la igualdad demostrada (1). ∎

En el § 2 del cap. 2 fue introducido el signo de la suma $\sum x_i$. Evidentemente, se puede utilizar en cualquier monoide conmutativo aditivo. En un monoide multiplicativo, de análogo sirve el signo de producto múltiple:

$$\prod_{i=1}^{2} x_i = x_1x_2, \quad \prod_{i=1}^{3} x_i = (x_1x_2)x_3, \quad \prod_{i=1}^{n} x_i = \left(\prod_{i=1}^{n-1} x_i\right)x_n.$$

En virtud del teorema 1, cuando se escribe (o cuando se calcula) el producto de los elementos $x_1x_2 \ldots x_n$ de un monoide, los paréntesis son superfluos. La única preocupación debe de manifestarse con respecto al orden de los multiplicadores, y sólo en el caso cuando no todos ellos son permutables entre sí. En particular, cuando $x_1 = x_2 = \ldots = x_n = x$, el producto $xx \ldots x$ se indica, al igual que cuando se opera con números, con el símbolo x, llamándolo n-ésima *potencia del elemento* x. Un corolario del teorema 1 resultan las relasiones

$$x^m x^n = x^{m+n}, \quad (x^m)^n = x^{mn}, \quad m, n \in \mathbb{N} \qquad (2)$$

En el monoide $(M, \cdot, e)$, para todo $x \in M$ también suponen $x^0 = e$.

A las potencias $x^n \in M, \cdot, e)$ en el monoide $(M, +, 0)$ les corresponden los *múltiplos* $nx = x + x + x \ldots + x$ del elemento x. Las reglas (2) pasan a ser reglas para los múltiplos:

$$mx + nx = (m + n)x, \quad n(mx) = (nm)x. \qquad (2')$$

Mencionemos otro hecho útil. Si $xy = yx$ en el monoide M, entonces

$$(xy)^n = x^n y^n, \quad n = 0, 1, 2, \ldots \qquad (3)$$

En particular, esto es siempre así en un monoide conmutativo. La relación (3) se demuestra por inducción en n:

$$(xy) = (xy)^{n-1}xy = (x^{n-1}y^{n-1})(xy) = (x^{n-1}y^{n-1}x)\,y =$$
$$= (x^{n-1}xy^{n-1})\,y = (x^{n-1}x)(y^{n-1}y) = x^ny^n$$

De forma más general, apoyándose en la relación (3) y utilizando la inducción sobre m, obtenemos

$$x_ix_j = x_jx_i,\ 1 \leqslant i,\ j \leqslant m \Rightarrow (x_1 \ldots x_m)^n = x_1^n \ldots x_m^n \qquad (4)$$

Análogamente,

$$n\,(x + y) = nx + ny, \qquad n = 0,\ 1,\ 2,\ \ldots, \qquad (3')$$

$$n\,(x_1 + \ldots + x_m) = nx_1 + \ldots + nx_m,\ n = 0,\ 1,\ 2,\ \ldots \qquad (4')$$

Habitualmente, al monoide $(M, \cdot, e)$ lo llaman *multiplicativo*, y al $(M, +, 0)$, *aditivo*. La escritura aditiva se utiliza preferentemente en los monoides conmutativos.

4. Elementos invertibles. El elemento a del monoide (M, , e) se llama *invertible*, si se halla un elemento $b \in M$, para el cual se cumple $ab = e = ba$ (se entiende, que el elemento b también será invertible). Si también $ab' = e = b'a$, entonces, $b' = eb' = (ba)\,b' = b\,(ab') = be = b$. Esto nos da fundamento para hablar sencillamente del *elemento inverso* a^{-1} al elemento (invertible) $a \in M$: $a^{-1}a = e = aa^{-1}$.

Se sobreentiende, que $(a^{-1})^{-1} = a$. El concepto de elemento invertible de un monoide sirve, evidentemente, para generalizar naturalmente el concepto de matriz invertible en el monoide multiplicativo $(M_n\,(\mathbb{R}), \cdot, E)$.

Como $(xy)(y^{-1}x^{-1}) = x\,(yy^{-1})\,x^{-1} = xex^{-1} = xx^{-1} = e$ y, análogamente, $(y^{-1}x^{-1})(xy) = e$, entonces, $(xy)^{-1} = y^{-1}x^{-1}$. Por consiguiente, *el conjunto de todos los elementos invertibles del monoide $(M, \cdot, e)$ es cerrado con respecto a la operación $\cdot$ y compone un submonoide en M.*

EJERCICIOS

1. En el punto 1, en calidad de ejemplo, se introdujo en $\mathbb{Z}$ la operación*: $n * m = -n - m$, conmutativa, pero no asociativa. En el sistema algebraico $(\mathbb{Z}, *)$ se cumplen las relaciones: $(n * m) * m = n$, $m * (m * n) = n$. Sea, que ahora nos es dado un sistema algebraico arbitrario $(X, *)$, en el cual $(x * y) * y = x$, $y * (y * x) = x$, para cualesquiera $x, y \in X$. De mostrar, que $x * y = y * x$, o sea, que la operación $*$ es conmutativa. (No se dan indicaciones para su resolución, por cuanto este ejercicio es uno de los más inútiles del libro. ¡Sin embargo!)

2. Mostrar, que

$$M_n^0\,(\mathbb{R}) = \{A = (a_{ij}) \in M_n\,(\mathbb{R}) \mid \sum_{j=1}^{n} a_{ij} = 0,\quad i = 1,\ 2,\ \ldots,\ n\}$$

es un semigrupo con la operación corriente de multiplicación de matrices. ¿Es o no $(M_n^\circ(\mathbb{R}), *)$ un monoide?

3. En el monoide multiplicativo M se elige un elemento arbitrario t y se introduce una nueva operación $*$: $x * y = xty$. Mostrar, que $(M, *)$ es un semigrupo y que la inversión del elemento t en M es la condición necesaria y suficiente, con cuyo cumplimiento, $(M, *)$ resulta un monoide con elemento neutro (unidad) t^{-1}.

4. Mostrar, que el conjunto $\mathbb{Z}$ con la operación $\circ$: $n \circ m = n + m + nm = (1 + n)(1 + m) - 1$, es un monoide conmutativo. ¿Qué sirve en $(\mathbb{Z}, \circ)$ de elemento neutro? Hallar en $(\mathbb{Z}, \circ)$ todos los elementos invertibles.

§ 2. GRUPOS

1. Definición y ejemplos. Examinemos el conjunto GL $(n, \mathbb{R})$ de todas las $n \times n$-matrices cuadradas con coeficientes reales, y con determinantes distintos de cero. Según el teorema 5 del § 2 del cap. 3, $\det A \neq 0$, $\det B \neq 0 \Rightarrow \det AB \neq 0$. Vemos, que $A, B \in$ GL $(n, \mathbb{R}) \Rightarrow AB \in$ GL $(n, \mathbb{R})$; luego, $(AB)C = A(BC)$, y existe una matriz escogida E tal, que $AE = EA = A$, para toda $A \in$ GL $(n, \mathbb{R})$. Además, cada matriz $A \in$ GL $(n, \mathbb{R})$ tiene su «antípoda», la matriz inversa A^{-1}, para la cual $AA^{-1} = A^{-1}A = E$.

El conjunto GL $(n, \mathbb{R})$, examinado junto con la ley de composición (operación binaria) $(A, B) \mapsto AB$ y llamado *grupo lineal completo de potencia n* sobre $\mathbb{R}$, se podría haber definido brevemente, siguiendo la terminología del § 1, como un submonoide de todos los elementos invertibles del monoide $(M_n(\mathbb{R}), \cdot, E)$. Pero este submonoide es tan importante, que se merece un nombre especial y brinda un argumento sólido para introducir una general

DEFINICION. El monoide G, todos los elementos del cual son inver bles, se llama *grupo*. En otras palabras, se presupone el cumpim iento de los siguientes axiomas:

(G1) *en el conjunto G está definida la operación binaria*: $(x, y) \mapsto xy$;

(G2) *la operación es asociativa*: $(xy)z = x(yz)$, *para todos lo* $x, y, z \in G$;

(G3) G *posee el elemento neutro* (*unidad*) e: $xe = ex = x$ *para todo* $x \in G$;

(G4) *para cada elemento* $x \in G$, *existe el inverso* x^{-1}: $xx^{-1} = x^{-1}x = e$.

Es admirable, que una de las ramas del álgebra más vieja y más rica en resultados, que juega un papel fundamental en la geometría y en las aplicaciones de las matemáticas a cuestiones de las ciencias naturales, se base en axiomas tan sencillos. Un pequeño análisis muestra, que se pueden simplificar aún más, pero esta tarea no es tan importante para nosotros.

Los grupos con operaciones conmutativas se llaman, naturalmente, conmutativos, y más frecuentemente, *abelianos* (en honor del matemático noruego Abel). El propio término «grupo» pertenece

al matemático francés Galois, el legítimo creador de la teoría de los grupos. La idea de teoría de los grupos «flotaba en el aire» (como frecuentemente sucede con las ideas matemáticas fundamentales) mucho antes de Galois, y algunos de sus teoremas ya habían sido demostrados en forma ingenua por Lagrange. Los trabajos geniales de Galois resultaron incomprendidos, y el renacimiento del interés por ellos comenzó sólo después del libro de Jordan «Curso de la teoría de permutaciones y de ecuaciones algebraicas» (año 1870). Sólo hacia fines del s. XIX en la teoría de los grupos «se renuncia totalmente a la fantasía. A cambio de esto, se prepara cuidadosamente el esqueleto lógico» (F. Klein, «Lecciones sobre el desarrollo de las matemáticas en el siglo XIX»).

Para la designación del número de los elementos en el grupo G (más exactamente, de la potencia del grupo) se utilizan los símbolos equivalentes Card G, $|G|$ o $(G:e)$. Casi todo lo dicho en el § 1 sobre los monoides se traslada a los grupos. Sólo corresponde realizar el cambio debido de palabras. En particular, el subconjunto $H \subset G$ se llama *subgrupo* en G, si $e \in H$; $h_1, h_2 \in H \Rightarrow h_1h_2 \in H$ y $h \in H \Rightarrow h^{-1} \in H$. El subgrupo $H \subset G$ *es propio*, si $H \neq e$ y $H \neq G$.

Aportamos algunos ejemplos de grupos:

1) En el grupo lineal completo $GL(n, \mathbb{R})$ ya conocido por nosotros, examinemos el subconjunto $SL(n, \mathbb{R})$ de matrices con determinante 1:

$$SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) \mid \det A = 1.$$

Es evidente, que $E \in SL(n, \mathbb{R})$. De acuerdo con los resultados generales del cap. 3 acerca de los determinantes, $\det A = 1$, $\det B = 1 \Rightarrow \det AB = 1$ y $\det A^{-1} = (\det A)^{-1} = 1$. Por eso, $SL(n, \mathbb{R})$ es un subgrupo en $GL(n, \mathbb{R})$; que lleva el nombre de *grupo lineal especial de potencia n* sobre $\mathbb{R}$. También lo llaman grupo *unimodular*, aunque a esto último frecuentemente se le incorporan matrices con determinante ± 1.

Hay que decir, que el grupo $GL(n, \mathbb{R})$, al ser receptáculo de muchos grupos interesantes, resulta para los matemáticos de distintas generaciones, como una fuente inagotable de nuevas ideas y de problemas no resueltos.

2) Empleando números racionales en lugar de los reales, llegaremos al grupo lineal completo $GL(n, \mathbb{Q})$ de potencia n sobre $\mathbb{Q}$ y a su subgrupo $SL(n, \mathbb{Q})$. A su tiempo $SL(n, \mathbb{Q})$ contiene al interesante subgrupo $SL(n, \mathbb{Z})$ de matrices enteras con determinante 1. El teorema 1 del § 3 del cap. 3, que propone una fórmula explícita para los coeficientes de la matriz inversa, muestra, que $SL(n, \mathbb{Z})$ es realmente un grupo. Los grupos $SL(n, \mathbb{Q})$ y $SL(n, \mathbb{Z})$ ocupan un lugar de honor en la teoría de los números. El conjunto parcialmente ordenado de los subgrupos examinados (véase el punto 3 del § 6 del cap. 1) del grupo $GL(n, \mathbb{R})$, se representa en el diagrama aquí ubicado (fig. 11).

3) Haciendo en los ejemplos 1) y 2) $n = 1$, llegamos, primero, a los grupos multiplicativos $\mathbb{R}^* = \mathbb{R} \setminus \{0\} = GL(1, \mathbb{R})$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\} = GL(1, \mathbb{Q})$ de los números reales y racionales. Estos grupos, evidentemente, son infinitos. Como en $(\mathbb{Z}, \cdot, 1)$ los únicos elementos invertibles son 1 y -1, entonces, $GL(1, \mathbb{Z}) = \{\pm 1\}$. Luego, $SL(1, \mathbb{R}) = SL(1, \mathbb{Q}) = SL(1, \mathbb{Z}) = 1$. Pero ya para $n = 2$ el grupo $SL(2, \mathbb{Z})$ es infinito: ya que le pertenecen, por ejemplo, todas las matrices

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}, \quad \begin{pmatrix} m & m-1 \\ 1 & 1 \end{pmatrix}, \quad m \in \mathbb{Z}.$$

Notemos también los grupos infinitos aditivos:

$$(\mathbb{R}, +, 0), \quad (\mathbb{Q}, +, 0), \quad \mathbb{Z}, +, 0).$$

4) Sean, Ω un conjunto arbitrario, y S (Ω) el conjunto de todas las transformaciones biyectivas (recíprocamente unívocas) f: $\Omega \to \Omega$. Volviendo a los resultados del § 5 del cap. 1 sobre las aplicaciones de conjuntos (teoremas 1, 2 y consecuencia del teorema 2) inmediatamente concluimos que S (Ω) es un grupo con una operación binaria natural, una composición de transformación. Se

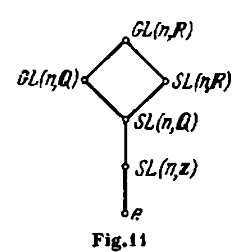


Fig. 11

sobreentiende, que S (Ω) es el submonoide de todos los elementos invertibles del monoide MΩ) del ejemplo 1) del § 1, pero no somos propensos a destacar esta circunstancia. Por sí mismo, el grupo S (Ω) y en particular, sus distintos subgrupos, llamados *grupos de transformación*, es la pista de despegue, de la cual comienzan todas las posibles aplicaciones de la teoría de los grupos. Es suficiente citar el famoso «programa de Erlangen» de F. Klein (1872) que puso el concepto de grupos de transformación como la base para clasificar los distintos tipos de geometrías. Tomando como el espacio lineal $\mathbb{R}^n$, llegaremos al «gran» y poco observable grupo S ($\mathbb{R}^n$). Pero en S ($\mathbb{R}^n$) está contenido el subgrupo de las transformaciones lineales invertibles (biyectivas) φ_A: $\mathbb{R}^n \to \mathbb{R}^n$, que se encuentran en correspondencia unívoca recíproca con la matriz no degenerada A de orden n (véase el § 3 del cap. 2).

De este modo, se obtiene la inclusión de GL (n, $\mathbb{R}$) en S ($\mathbb{R}^n$).

El sentido de esta inclusión resultará más claro cuando se introduzca el concepto fundamental de isomorfismo de los grupos.

2. Sistema de generadores (este punto, en una primera lectura, puede omitirse).

Teniendo un subconjunto S del grupo G, probemos elegir un subgrupo $H \subset G$, contenedor de S y tal, que para todo subgrupo $K \subset G$ de $S \subset K$ se inferirá la inclusión $H \subset K$. No puede ser que existan dos subgrupos mínimos H, H' de género semejante:

$$S \subset H, \ S \subset H' \Rightarrow H \subset H' \subset H \Rightarrow H' = H'.$$

Así que el subgrupo mínimo H debe coincidir con la intersección de todos los subgrupos, contenedores de S, si es que esta intersección resulta subgrupo en G. Mas tiene lugar el sencillo

TEOREMA 1. *La intersección* $\bigcap_{i \in I} H_i$ *de cualquier familia de subgrupos* $\{H_i \mid i \in I\}$ *del grupo* G, *es un subgrupo.*

DEMOSTRACIÓN. Sea e el elemento unidad del grupo G. Las propiedades $e \in \bigcap H_i$; $x, y \in \bigcap H_i \Rightarrow xy \in \bigcap H_i$; $x \in \bigcap H_i \Rightarrow x^{-1} \in \in \bigcap H_i$, que caracterizan a todo subgrupo, son cumplidas en $\bigcap H_i$, por eso, se cumplen en cada uno de los subgrupos H_i por separado. ∎

Tomemos ahora en calidad de familia $\{H_i \mid i \in I\}$ los mismos subgrupos, que contienen al subconjunto dado $S \subset G$. Entonces, su intersección

$$\langle S \rangle = \bigcap_{S \subseteq H} H$$

en virtud del teorema 1 y de las observaciones anteriormente efectuadas, será precisamente un subgrupo mínimo, contenedor de S. Llamamos al subgrupo $\langle S \rangle$ *engendrado* por el conjunto S en el grupo G, y a S, conjunto de *generadores* del subgrupo $\langle S \rangle$. A primera vista, $\langle S \rangle$ no se formula eficazmente, porque es necesario revisar todos los subgrupos contenedores de S. Sin embargo, no hay necesidad de ello, como lo muestra la sencilla afirmación que se deduce del teorema 1.

COROLARIO. *El subgrupo $\langle S \rangle \subset G$ coincide con el conjunto T, compuesto del elemento unidad e y de todos los productos posibles*

$$t_1 t_2 \ldots t_n, \quad n = 1, 2, 3, \ldots$$

donde, o $t_i \in S$, o bien $t_i^{-1} \in S$, $1 \leqslant i \leqslant n$.

Efectivamente, como $t_1 \ldots t_n \in T$, $t'_1 \ldots t'_m T \Rightarrow t''_1 \ldots \ldots t''_{n+m} = t_1 \ldots t_n t'_1 \ldots t'_m \in T$ y $t_1 \ldots t_n \in T \Rightarrow (t_1 \ldots \ldots t_n)^{-1} = t_n^{-1} \ldots t_1^{-1} \in T$, entonces, el conjunto T es subgrupo en G. Por otro lado, cada subgrupo H, contenedor de todos los $x_i \in S$, debe contener a todos los inversos x_i^{-1} y, por lo tanto, a todos los productos del tipo $t_1 t_2 \ldots t_n$. Por eso $H \supset T$, y T coincide con la intersección de todos esos subgrupos.

Hay que hacer notar, que falta mucho para que todos los productos $t_1 t_2 \ldots t_n$ sean distintos elementos del subgrupo $\langle S \rangle$, incluso si se conviene (lo que es natural) en reemplazar a los pares que se encuentren de elementos recíprocamente inversos aa^{-1}, $a^{-1}a$, por el elemento unidad. En general, para $|S| > 1$, la cuestión de la igualdad de los productos $t_1 t_2 \ldots t_n$ es difícil y será brevemente tratada recién en el cap. 7.

Cada grupo G es engendrado por algún sistema de generadores S: como S se puede tomar, por ejemplo, a todo el grupo G. Por simplicidad, examinemos el grupo G, engendrado por el conjunto finito S de sus elementos (tales grupos se llaman *engendrados finitos*). Eliminando de S los elementos «sobrantes», que se escriben en forma de producto de los que quedan (y sus inversos), llegamos al sistema *mínimo* de generadores M del grupo G. Esto significa, que $\langle M \rangle = G$, pero $\langle M' \rangle \neq G$, si el sistema M' es obtenido del M eliminando por

lo menos un elemento. Sea, digamos, $M = \{g_1, \ldots, g_d\}$. Entonces, en lugar de $G = \langle M \rangle$ se escribe también $G = \langle g_1, g_2, \ldots, g_d \rangle$. Cuando $d = 1$ se habla de grupo *cíclico*.

3. Grupos cíclicos. Si G es un grupo arbitrario y g su elemento, entonces, por definición, $\langle g \rangle$ es un subgrupo cíclico en G.

En concordancia con el teorema 1 y con las propiedades de las potencias de los elementos en los monoides, es natural esperar que todo grupo cíclico $\langle a \rangle$ con el generador a, resulta un grupo abeliano del tipo $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, o $\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$ (esta escritura no significa que todos los elementos a^n o na sean diferentes), de acuerdo a qué tipo de grupos examinemos, multiplicativo o aditivo. Así es, pero hay que convenir en la designación de $(a^{-1})^k = a^{-k}$ y demostrar la afirmación siguiente.

TEOREMA 2. *Cualesquiera que fueran* m, $n \in \mathbb{Z}$,

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{m n}$$

(correspondientemente, $ma + na = (m+n)\,a$, $n\,(ma) = (nm)\,a$*).*

DEMOSTRACION. Para m, n no negativos, véanse las relaciones (2), (2′) en el punto 4 del § 1. Si $m < 0$, $n < 0$, entonces $m' = -m > 0$, $n' = -n > 0$, y

$$a^m a^n = (a^{-1})^{m'} (a^{-1})^{n'} = (a^{-1})^{m'+n'} = a^{-(m'+n')} = a^{m+n}.$$

Para $m' = -m > 0$, $n > 0$, tenemos

$$a^m a^n = (a^{-1})^{m'} a^n = \underbrace{(a^{-1} \ldots a^{-1})}_{m'} \underbrace{(a \ldots a)}_{n'} =$$

$$= a^{n-m'} \left(\text{o } (a^{-1})^{m'-n}, \text{ si } m' \geqslant n\right) = a^{m+n}.$$

Análogamente se examina el caso cuando $m > 0$, $n < 0$. La igualdad $(a^m)^n = a^{mn}$ se deduce de lo anterior y es suficientemente evidente por definición de potencia. ■

Un ejemplo sencillísimo de grupo cíclico es el grupo aditivo de números enteros $(\mathbb{Z}, +, 0)$, generado por la unidad ordinaria 1 o -1. Es fácil verificar, que la matriz $\begin{Vmatrix} 1 & 0 \\ 1 & 1 \end{Vmatrix}$ genera en SL $(2, \mathbb{Z})$ un subgrupo cíclico infinito. El conjunto $\{1, -1\}$ es un grupo cíclico de orden 2 por multiplicación.

Un ejemplo de grupo cíclico de orden n se obtiene, si se examinan todas las rotaciones en un plano, alrededor de algún punto O, de una figura n-angular regular P_n coincidente con el plano y con centro en el punto O. Evidentemente, estas rotaciones generan un grupo; como sus productos, cabe entender el cumplimiento sucesivo de transformaciones. Nuestro grupo C_n contiene rotaciones $\varphi_0, \varphi_1, \ldots, \varphi_{n-1}$ en sentido opuesto a las agujas de un reloj, en ángulos iguales a $0, \frac{2\pi}{n}, \ldots, (n-1)\frac{2\pi}{n}$. Además, $\varphi_s = \varphi_1^s$, y por reflexiones geométricas se ve, que $\varphi_s^{-1} = \varphi_1^{n-s}$ y $\varphi_1^n = \varphi_0$ (transformación unitaria). Así

pues, $|C_n| = n$ y $C_n = \langle\varphi_1\rangle$. Observemos, que el grupo cíclico C_n es un subgrupo propio del grupo D_n de todas las transformaciones de simetría de la figura n-angular P_n (o sea, coincidencia de P_n consigo mismo).

Sean, de nuevo, un grupo arbitrario G y algún elemento del mismo a. Hay dos posibilidades: 1) todas las potencias de a son distintas, o sea $m \neq n \Rightarrow a^m \neq a^n$. En este caso, se dice que el elemento $a \in G$ *tiene un orden infinito*. 2) Se tienen coincidencias $a^m = a^n$, para $m \neq n$. Si, por ejemplo, $m > n$, entonces, $a^{m-n} = e$, o sea, existen potencias positivas del elemento $a \in G$, iguales al elemento unidad. Sea q el menor exponente positivo, para el cual $a^q = e$. Entonces, se dice, que a es un elemento *de orden finito q*. En el grupo finito G (Card $G < \infty$) todos los elementos, por supuesto, serán de orden finito.

Advertencia. La palabra «orden» en matemáticas, tiene significados múltiples. Antes hablamos de matrices cuadradas de orden n (matrices de dimensiones $n \times n$), pero la matriz no degenerada A, considerada como elemento del grupo GL $(n, \mathbb{R})$ tiene también un orden (posiblemente infinito) en el sentido recién indicado. En cada caso, surgirá claramente del contexto a qué orden nos referimos.

En el marco del ejemplo, dado arriba, de grupo cíclico de orden n, la siguiente afirmación es casi evidente.

TEOREMA 3. *El orden de cualquier elemento $a \in G$ (G es un grupo abstracto) es igual a Card $\langle a\rangle$. Si a es un elemento de orden finito q, entonces*

$$\langle a\rangle = \{e, a, \ldots, a^{q-1}\} \text{ y } a^k = e \Leftrightarrow k = lq, \ l \in \mathbb{Z}.$$

DEMOSTRACION. En el caso de un elemento de orden infinito, no hay nada que demostrar. Si a es de orden q, entonces, por definición, todos los elementos $e, a, a^2, \ldots, a^{q-1}$ son distintos. Cualquiera otra potencia a^k coincide con uno de estos elementos, o sea $\langle a\rangle = \{e, a, \ldots, a^{q-1}\}$. En efecto, usándose el algoritmo de división en $\mathbb{Z}$ (punto 3 del § 8 del cap. 1), escribimos el exponente k de la forma

$$k = lq + r, \ 0 \leqslant r \leqslant q - 1,$$

luego de lo cual, operando con potencias de acuerdo a las reglas expuestas en el teorema 2, obtenemos

$$a^k = (a^q)^l a^r = ea^r = a^r.$$

En particular, $a^k = e \Rightarrow r = 0 \Rightarrow k = lq$. ∎

La propiedad cíclica de un grupo, muy útil y cómodo, no siempre es dada apriori: a veces, hay que demostrarla. En calidad de ejemplo, consideremos la siguiente

PROPOSICION. *Los elementos permutados a, b, del grupo arbitrario G, que tienen órdenes s, t primos entre sí, generan en G un subgrupo cícli-*

co de orden st

$$\langle a, b\rangle = \langle ab\rangle.$$

DEMOSTRACION. En efecto, $D = \langle a\rangle \cap \langle b\rangle = e$, por cuanto, para todo elemento $d \in D$, que tenga algún orden q, por el teorema 3, tenemos

$$d = a^i = b^j \Rightarrow d^s = (a^s)^i = e, \quad d^t = (b^t)^j = e \Rightarrow q \mid s, q \mid t,$$

y como s, t son primos entre sí, se deduce que $q = 1$. Si, además, $n = |\langle ab\rangle|$, entonces (véase la relación (3) del § 1),

$$a^n b^n = (ab)^n = e \Rightarrow a^n = b^{-n} \in D = e \Rightarrow a^n = e, b^n = e \Rightarrow$$
$$\Rightarrow s \mid n, t \mid n \Rightarrow \text{m.c.m. } (s, t) \mid n \Rightarrow st \mid n,$$

por cuanto, $st =$ m.c.m. (s, t) m.c.d. (s, t). Pero $(ab)^{st} = (a^s)^t (b^t)^s = e$ (teorema 2), así que $n \mid st$ y, en consecuencia, $n = st$. Queda por observar, que

$$\langle a, b\rangle = \{a^i b^j \mid 0 \leqslant i \leqslant s-1, \quad 0 \leqslant j \leqslant t-1\} \Rightarrow \text{Card } \langle a, b\rangle \leqslant st,$$

y como, $\langle ab\rangle \subset \langle a, b\rangle$ y Card $\langle ab\rangle = st$, entonces, $\langle a, b\rangle = \langle ab\rangle$. ∎

Aún volveremos a los grupos cíclicos, pero ahora examinemos más fundamentalmente un tipo especial de grupos de transformaciones, en los cuales se ilustran en forma muy evidente los conceptos introducidos.

4. Grupos simétricos y alternados. Sea Ω un conjunto finito de n elementos. Puesto que la naturaleza de los elementos para nosotros no es esencial, es cómodo considerar que $\Omega = \{1, 2, \ldots, n\}$. El grupo $S(\Omega)$ (véase el ejemplo 4, dado anteriormente), de todas las aplicaciones biunívocas $\Omega \to \Omega$ se llama *grupo simétrico de grado n* (de otro modo: *grupo simétrico en n símbolos*, o *en n puntos*) y muy frecuentemente es designado por medio de S_n.

Sus elementos, por lo común designados con letras griegas minúsculas, se llaman *permutaciones*.

Observación. A veces, los elementos del grupo S_n se denominan sustituciones, utilizando el término «permutación» como sinónimo de una disposición de los números 1, 2, . . ., n en cierto orden fijado. Como entre los ordenamientos de los números y los elementos del grupo S_n existe una correspondencia biunívoca, y la palabra «permutación» conscientemente se asocia más bien a una acción que a un ordenamiento fijo, entonces, las sustituciones quedan excluidas de nuestro uso. Por otra parte, posteriormente, por ejemplo, hablaremos sobre la sustitución de un número en un polinomio, pero esto sirve solamente de argumento complementario en favor del acuerdo terminológico indicado.

Si se necesitan algunos argumentos más, se pueden hallar en la literatura científica.

En forma desarrollada y explícita, la permutación π: $i \mapsto \pi(i)$, $i = 1, 2, \ldots, n$, se representa con el símbolo de dos filas

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

que indica totalmente todas las imágenes

$$\pi: \begin{matrix} 1 & 2 & \dots & n \\ \downarrow & \downarrow & & \downarrow \\ i_1 & i_2 & \dots & i_n \end{matrix},$$

donde $i_k = \pi(k)$, $k = 1, \dots, n$, son los símbolos permutados $1, 2, \dots, n$. Como siempre, e es la permutación unidad (aunque es letra del alfabeto latino): $e(i) = i$, $\forall i$.

Las permutaciones $\sigma, \tau \in S_n$ se multiplican de acuerdo con la regla general de composición de aplicaciones $(\sigma\tau)(i) = \sigma(\tau(i))$. Por ejemplo, para la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

tenemos

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 2 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 2 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

Al mismo tiempo

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

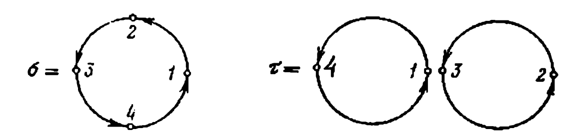
así que $\sigma\tau \neq \tau\sigma$.

A veces, junto con el grupo G es cómodo examinar el llamado grupo *opuesto*. Si G es un grupo en relación a la operación binaria $\circ$: $(f, g) \to f \circ g$, entonces, es también un grupo respecto a la operación $*$: $(f, g) \to g \circ f$. El grupo con operación contraria se designa G^{op}. Este hecho refleja la simetría de los axiomas de grupos, en los que se habla de inversos bilaterales y de unidades bilaterales. El axioma de asociatividad también es simétrico. En particular, en el grupo S_n^{op} se establece la regla de multiplicación de dos permutaciones, en el sentido corriente de izquierda a derecha. Si hubiéramos escrito $i\sigma$ o i^σ en lugar de $\sigma i = \sigma(i)$, entonces, esto también hubiese sido habitual para nosotros.

Hallemos el orden del grupo S_n. Con la permutación σ, el símbolo 1 se puede llevar a otro cualquiera $\sigma(1)$, para lo que existen, exactamente, n posibilidades distintas. Pero, fijando a $\sigma(1)$, tenemos derecho de elegir en calidad de $\sigma(2)$ solamente a uno de los $n - 1$ símbolos restantes (en total, pares distintos de $\sigma(1)$, $\sigma(2)$, se tienen $(n-1) + (n-1) + \dots + (n-1) = n(n-1)$, en calidad de $\sigma(3)$, respectivamente $n - 2$ símbolos, etc. El total de las elecciones posibles $\sigma(1), \sigma(2), \dots, \sigma(n)$, y, por consiguiente, de todas las permutaciones posibles, resulta $n(n-1) \dots 2\cdot 1 = n!$ (factorial de n). De este modo,

$$\text{Card } S_n = |S_n| = (S_n : e) = n!.$$

Descomponemos ahora las permutaciones de S_n en productos de permutaciones más simples. La idea de la descomposición la explicamos esquemáticamente en el ejemplo de las permutaciones anteriormente mencionadas σ, $\tau \in S_4$:



La permutación σ, brevemente se escribe en forma $\sigma = (1234)$ o, lo que es lo mismo, en forma $\sigma = (2341) = (3412) = (4123)$, y lleva el nombre de *ciclo* de longitud 4, mientras la permutación $\tau = (14)(23)$, es el producto de dos *ciclos independientes* (*no intersecados*) (14) y (23) de longitud 2. Observemos, que $\sigma^2 = (13)(24)$, $\sigma^4 = (\sigma^2)^2 = e$, $\tau^2 = e$.

Pasando al caso general, llamamos a dos puntos $i, j \in \Omega$ *equivalentes* respecto al subgrupo cíclico $\langle\pi\rangle \subset S_n$, o sencillamente π-*equivalentes*, si $j = \pi^s(i) = \pi(\ldots \pi(i) \ldots)$ para algún $s \in \mathbb{Z}$. Como S_n es un grupo finito, entonces, cada uno de sus subgrupos también es finito. Por el teorema 3, en el caso en que Card $\langle\pi\rangle = q$, se puede considerar que $0 \leqslant s < q$. Estamos en presencia de relaciones reflexivas, simétricas y transitivas (véase el punto 2, del § 6 del cap. 1), por cuanto $i = \pi^0(i) = e(i)$; $j = \pi^h(i) \Rightarrow i = \pi^{-h}(j)$ y $j = \pi^s(i)$, $k = \pi^t(j) \Rightarrow k = \pi^{s+t}(i)$. En correspondencia con la propiedad general de relaciones de equivalencia, obtenemos la partición

$$\Omega = \Omega_1 \cup \ldots \cup \Omega_p \qquad (1)$$

del conjunto Ω, en clases $\Omega_1, \ldots, \Omega_p$, disjuntas de dos en dos, a las que se acostumbra llamar también π-*órbitas*. Este nombre está plenamente justificado. Cada punto $i \in \Omega$ pertenece exactamente a una órbita, y si $i \in \Omega_k$, entonces Ω_k está compuesto de imágenes del punto i con la operación de potencias del elemento π: i, $\pi(i)$, $\pi^2(i), \ldots, \pi^{l_k-1}(i)$. Aquí, $l_k = |\Omega_k|$ es la longitud de la π-órbita de Ω_k. Evidentemente, $l_k \leqslant q = \text{Card}\langle\pi\rangle$ y $\pi^{l_k}(i) = i$, además, l_k es el menor número que posee esta propiedad. Haciendo

$$\pi_k = (i\pi(i) \ldots \pi^{l_k-1}(i)) = \begin{pmatrix} i & \pi(i) & \ldots & \pi^{l_k-2}(i) \\ \pi(i) & \pi^2(i) & \ldots & \pi^{l_k-1}(i) \end{pmatrix},$$

llegamos, precisamente, a la permutación llamada ciclo de longitud l_k.

Es cuestión de gusto y comodidad, escribir $(123 \ldots l)$ o $(1, 2, 3, \ldots, l)$, separando los símbolos con comas. El ciclo π_k deja en su lugar a todos los puntos del conjunto $\Omega \setminus \Omega_k$, y $\pi(j) = \pi_k(j)$ para cualquier punto $j \in \Omega_k$. Esta propiedad nos da pie para llamar a los π_s, π_t, $s \neq t$, ciclos *independientes o disjuntos*. Como $\pi^{l_k}(i) = i$ para $i \in \Omega_k$, entonces, $\pi_k^{l_k} = e$.

Así que, con la partición (1) se asocia la descomposición de la permutación π en el producto

$$\pi = \pi_1 \pi_2 \ldots \pi_p, \tag{2}$$

donde todos los ciclos son permutados: $\pi = \pi_1\pi_2 \ldots \pi_p = \pi_{i_1}\pi_{i_2} \ldots \pi_{i_p}$.

Se puede considerar, por ejemplo, que $l_1 \geqslant l_2 \geqslant \ldots \geqslant l_m > l_{m+1} = \ldots = l_p = 1$.

Si el ciclo $\pi_k = (i)$ tiene una longitud 1, entonces, opera como una permutación unitaria; es natural omitir tales ciclos en el producto (2):

$$\pi = \pi_1\pi_2 \ldots \pi_m; \quad l_k > 1, \quad 1 \leqslant k \leqslant m. \tag{3}$$

Por ejemplo, la permutación

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} \in S_8$$

la escribimos de forma

$$\pi = (12345)(67)(8) = (12345)(67). \tag{4}$$

Alguna dificultad provoca el hecho de que (12345) (67) puede ser interpretada como una permutación de S_n para cualquier $n \geqslant 7$, sin embargo, cuando n está dado, no hay ninguna ambivalencia.

Más exactamente, sea que junto con la descomposición (3), tenemos otra descomposición $\pi = \alpha_1\alpha_2 \ldots \alpha_r$ en productos de ciclos independiente, además sea i un símbolo que, cuando se efectúa la operación π, no queda en su lugar. Entonces, $\pi_s(i) \neq i$, $\alpha_t(i) \neq i$ para uno (y sólo para uno) de los ciclos $\pi_1, \ldots, \pi_m$ y para uno de los $\alpha_1, \ldots, \alpha_r$. Tenemos

$$\pi_s^k(i) = \pi^k(i) = \alpha_t^k(i), \quad k = 0, 1, 2, \ldots$$

Pero un ciclo se determina unívocamente por la operación de su potencia sobre cualquier símbolo, que no se conserve en su lugar. En consecuencia, $\pi_s = \alpha_t$. Más adelante se aplica inducción sobre m o r.

Así, hemos demostrado el

TEOREMA 4. *Cada permutación $\pi \neq e$ en S_n, es un producto de ciclos independientes de longitud $\geqslant 2$. Esta descomposición en un producto está definida unívocamente, exactamente hasta el orden de recorrido de los ciclos.* ∎

La escritura compacta (3) de la permutación π, a la que se hace mención en el teorema 4, es cómoda por muchas razones. En particular, permite, encontrar fácilmente el orden de una permutación.

COROLARIO 1. *El orden de la permutación $\pi \in S_n$ (= al orden del subgrupo cíclico $\langle\pi\rangle$) es igual al mínimo común múltiplo de las longitudes de los ciclos independientes, que entran en la descomposición π.*

DEMOSTRACIÓN. Antes ya se observó que los ciclos independientes en la descomposición $\pi = \pi_1\pi_2 \ldots \pi_m$ son permutables, o, como también se dice, conmutan. Por eso, de acuerdo a la relación (4) del § 1,

$$\pi^s = \pi_1^s \ldots \pi_m^s, \quad s = 0, 1, 2, \ldots$$

Como los ciclos $\pi_1, \ldots, \pi_m$ son independientes (operan en distintos conjuntos $\Omega_1, \ldots, \Omega_m$), entonces, $\pi^q = e \Longleftrightarrow \pi_k^q = e$, para $k = 1, \ldots, m$. Luego, q es un múltiplo común de los ciclos π_k, los que, como vimos, coinciden con sus dimensiones l_k. Si q es el menor número natural, para el cual $\pi^q = e$, entonces, $q = \text{Card}\,\langle\pi\rangle$ y $q = \text{m.c.m.}\,(l_1, \ldots, l_m)$ es un número entero, definido en el punto 2, del § 8 del cap. 1. Véase también la frase al final del punto 3. ∎

Por ejemplo, inmediatamente podemos decir que, el orden de las permutaciones del tipo (4) es igual a 10. ¿Y cuál es el máximo orden de los elementos de S_8? Eligiendo las particiones del número 8 en sumandos positivos, dispuestos en orden no decreciente, llegamos a la conclusión, que los órdenes de los elementos $\neq e$ en S_8 son dados por los números enteros 2, 3, 5, 6, 7, 8, 10, 12, 15. En calidad de elemento de máximo orden 15 se puede tomar, por ejemplo, la permutación = (12345) (678).

DEFINICIÓN. El ciclo de longitud 2 se llama *trasposición.*

Cualquier trasposición tiene la forma $\tau = (ij)$ y deja en su lugar a todos los símbolos, distintos de i, j. Del teorema 4 se deduce el

COROLARIO 2. *Cada permutación $\pi \in S_n$ es producto de trasposiciones.*

En efecto, en virtud del teorema 4, es suficiente escribir en forma de productos de trasposiciones, cada uno de los ciclos. Pero esto se puede hacer, por ejemplo, así:

$$(12 \ldots l-1\ l) = (1l)\,(1\,l-1) \ldots (13)\,(12). \quad ∎$$

La afirmación del corolario 2 se puede expresar de otro modo, utilizando el concepto de sistemas generadores de grupos (véase el punto 2)

$$S_n = \langle (12), \ldots, (1n), (23), \ldots, (2n), \ldots, (n-1n) \rangle.$$

Por supuesto, este sistema de generadores no es mínimo. Por ejemplo

$$S_3 = \langle (12), (13), (23) \rangle = \langle (12), (13) \rangle.$$

En consecuencia, no se puede hablar de ninguna unicidad de escritura de una permutación por medio de trasposiciones: las trasposiciones,

hablando en general, no conmutan, y su número no es invariante de la permutación. Por ejemplo, en S_4 tenemos

$$(123) = (13)(12) = (23)(13) = (13)(24)(12)(14).$$

Por otra parte, la multiplicidad de la descomposición se aprecia de la igualdad $\sigma\tau^2 = \sigma$ para cualesquiera trasposiciones σ y τ. No obstante, un invariante de descomposición de permutaciones por medio de trasposición, pese a todo, existe. A fin de poder descubrirlo, en la medida de lo posible, de un modo natural, consideremos la operación S_n sobre las funciones.

DEFINICION. Sean, $\pi \in S_n$ y $f(X_1, \ldots, X_n)$, funciones de cualesquiera n argumentos. Suponemos

$$(\pi \circ f)(X_1, \ldots, X_n) = f(X_{\pi^{-1}(1)}, \ldots, X_{\pi^{-1}(n)}). \tag{5}$$

Se dice, que *la función $g = \pi \circ f$ se obtiene por operación de π sobre f.*

Por ejemplo, si $\pi = (123)$ y $f(X_1, X_2, X_3) = X_1 + 2X_2^2 + 3X_3^3$, entonces, $(\pi \circ f)(X_1, X_2, X_3) = X_3 + 2X_1^2 + 2X_2^3$.

En correspondencia con el § 1 del cap. 3, la función f se llama *antisimétrica*, si $\tau \circ f = -f$, para cualquier trasposición $\tau \in S_n$, o sea,

$$f(\ldots, X_j, \ldots, X_i, \ldots) = -f(\ldots, X_i, \ldots, X_j, \ldots).$$

LEMA. *Sean α, β dos permutaciones cualesquiera de S_n. Entonces*

$$(\alpha\beta) \circ f = \alpha \circ (\alpha \circ f).$$

DEMOSTRACION. En correspondencia con la relación definitoria (5) tenemos

$$((\alpha\beta) \circ f)(X_1, \ldots, X_n) = f(X_{(\alpha\beta)^{-1}(1)}, \ldots, X_{(\alpha\beta)^{-1}(n)}) =$$
$$= f(X_{(\beta^{-1}\alpha^{-1})(1)}, \ldots, X_{(\beta^{-1}\alpha^{-1})(n)}) = f(X_{\beta^{-1}(\alpha^{-1}1)}, \ldots, X_{\beta^{-1}(\alpha^{-1}n)}) =$$
$$= (\beta \circ f)(X_{\alpha^{-1}(1)}, \ldots, X_{\alpha^{-1}(n)}) = (\alpha \circ (\beta \circ f))(X_1, \ldots, X_n). \blacksquare$$

TEOREMA 5. *Sea π una permutación de S_n,*

$$\pi = \tau_1\tau_2 \ldots \tau_k \tag{6}$$

alguna descomposición de π en un producto de trasposiciones. Entonces, el número

$$\varepsilon_\pi = (-1)^k, \tag{7}$$

denominado paridad de π (o de otro modo: *signatura o signo de π*) *queda totalmente determinado por la permutación π y no depende del modo de descomposición* (5), *o sea, la paridad del número entero k, para la permutación dada π, es siempre la misma. Además,*

$$\varepsilon_{\alpha\beta} = \varepsilon_\alpha\varepsilon_\beta \tag{8}$$

para todos los α, $\beta \in S_n$.

DEMOSTRACION. Tomamos una función antisimétrica arbitraria f, de n argumentos $X_1, \ldots, X_n$. Por el lema, la operación de π sobre f se reduce a una sucesiva aplicación de trasposiciones τ_k,

$\tau_{k-1}, \ldots, \tau_1$, o sea, a k repetidas multiplicaciones de f por -1:

$$\pi \circ f = (\tau_1 \ldots \tau_{k-1}) \circ (\tau_k \circ f) =$$
$$= -(\tau_1 \ldots \tau_{k-1}) \circ f = \ldots = (-1)^k f = \varepsilon_\pi f.$$

Como el primer miembro de esta relación depende de π, pero no de ninguna de sus descomposiciones, entonces, y la aplicación $\varepsilon: \pi \to \varepsilon_\pi$, dada por la igualdad (7), debe determinarse totalmente por la permutación π con la condición, claro, de que f no sea una función idénticamente nula. Pero sabemos, que existen funciones antisimétricas distintas de cero; por ejemplo, el determinante de Vandermonde $\Delta_n (X_1, \ldots, X_n)$ de orden n.

La aplicación a una función f, de las permutaciones $\alpha\beta$ de acuerdo a la regla expuesta en el lema, da

$$\varepsilon_{\alpha\beta} f = (\alpha\beta) \circ f = \alpha \circ (\beta \circ f) = \alpha \circ (\varepsilon_\beta f) = \varepsilon_\beta (\alpha \circ f) =$$
$$= \varepsilon_\beta (\varepsilon_\alpha f) = (\varepsilon_\alpha \varepsilon_\beta) f,$$

de donde se obtiene la relación (8). ∎

DEFINICION. La permutación $\pi \in S_n$ se llama *par*, si $\varepsilon_\pi = 1$, e *impar*, si $\varepsilon_\pi = -1$.

De la definición se deduce, que *todas las trasposiciones son permutaciones impares.*

COROLARIO 1. *Todas las permutaciones pares de potencia n forman el subgrupo $A_n \subset S_n$ de orden $n!/2$ (se llama grupo alternado de potencia n).*

DEMOSTRACION. De acuerdo con (8), $\varepsilon_{\alpha\beta} = 1$, si $\varepsilon_\alpha = \varepsilon_\beta = 1$, y $\varepsilon_{\pi^{-1}} = \varepsilon_\pi$, por cuanto $\varepsilon_e = 1$. Como A_n es un subconjunto en S_n, entonces, todos los axiomas de grupo se cumplen.

Escribamos S_n en forma de unión $S_n = A_n \cup \bar{A}_n$, donde $\bar{A}_n$ es el conjunto de todas las permutaciones impares de potencia n. La aplicación de S en sí misma, definida por la regla

$$\rho_{12}: \pi \to (12)\,\pi,$$

es biyectiva. Es inyectiva: $(12)\,\alpha = (12)\,\beta \Rightarrow \alpha = \beta$; a continuación, empleando el teorema 3 del § 5 del cap. 1, se puede sencillamente notar, que $(\rho_{(12)})^2$ es una aplicación idéntica. Como $\varepsilon_{(12)\pi} = \varepsilon_{(12)}\varepsilon_\pi = -\varepsilon_\pi$, entonces, $\rho_{(12)} A_n = \bar{A}_n$, $\rho_{(12)}\bar{A}_n = A_n$. Quiere decir, que el número de permutaciones pares en S_n, coincide con el número de permutaciones impares, de donde $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$. ∎

COROLARIO 2. *Sea la permutación $\pi \in S_n$, descompuesta en un producto de ciclos independientes de longitudes $l_1, l_2, \ldots, l_m$.* Entonces

$$\varepsilon_\pi = (-1)^{\sum_{k=1}^{m}(l_k-1)}.$$

Efectivamente, según el teorema 5 tenemos $\varepsilon_\pi = \varepsilon_{\pi_1 \ldots \pi_m} = \varepsilon_{\pi_1} \ldots \varepsilon_{\pi_m}$. Además, $\varepsilon_{\pi_k} = (-1)^{l_k-1}$, por cuanto π_k se escribe en forma de producto de $l_k - 1$ trasposiciones (véase la demostración del corolario 2 del teorema 4). Definitivamente,

$$\varepsilon_\pi = (-1)^{l_1-1} \ldots (-1)^{l_m-1} = (-1)^{\sum_{k=1}^{m}(l_k-1)}. \blacksquare$$

Para finalizar, a fin de descansar de cosas serias, examinemos el conocido juego de «quince». Quince fichas cuadradas, planas, de igual medida, numeradas, se distribuyen en un tablero cuadrado, dividido en 16 campos de iguales dimen-

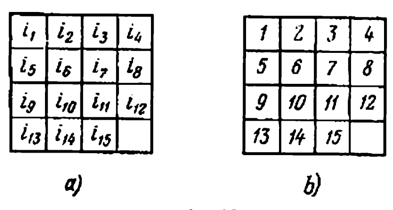


Fig. 12

siones que las fichas. Queda libre un campo, utilizando el cual, se pueden mover las fichas en forma horizontal o vertical (sin sacarlas del tablero). Se requiere, a partir de una distribución inicial, arbitraria, dada de las fichas (véase la fig. 12, a; en la posición inicial, se puede considerar campo libre al ángulo inferior derecho), pasar a una distribución correcta (véase la fig. 12, b). ¿Cuándo es posible dar este paso? La teoría elemental de los grupos «mató» a este juego en su pleno auge «de salón». Con las figuras a) y b) se asocia la permutación $\pi \in S_{15}$. No es difícil convencerse (de cualquier modo, se recomienda convencerse) de que la distribución correcta es alcanzable si, y sólo si, la paridad ε de la permutación π es igual a 1, o sea, si $\pi \in A_{15}$.

EJERCICIOS

1. Mostrar, que si $M = \langle S \rangle$ es un monoide, engendrado por el conjunto S y cada elemento $s \in S$ es invertible en M, entonces, M es un grupo.

2. Grupo, es un monoide G con elemento neutro, en el cual las ecuaciones del tipo $ax = b$, $ya = b$ tienen solución única para cualquier $a, b \in G$. Demostrar esta afirmación.

3. Mostrar, que el conjunto A_1 (R) de las llamadas *transformaciones afines* $\varphi_{a,b}: x \mapsto ax + b$ ($a, b \in \mathbb{R}$; $a \neq 0$) de la recta real $\mathbb{R}$, forma un grupo con ley de multiplicación $\varphi_{a,b}\varphi_{c,d} = \varphi_{ac,ad+b}$. En el grupo A_1 (R) está contenido el subgrupo de los «desplazamientos puros» $x \mapsto x + b$.

4. El grupo $SL(2, \mathbb{Z})$ contiene los elementos $A = \left\|\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}\right\|$, $B = \left\|\begin{matrix} 0 & 1 \\ -1 & -1 \end{matrix}\right\|$ de órdenes 4 y 3, respectivamente. Mostrar, que $\langle AB \rangle$ es un subgrupo cíclico infinito en $SL(2, \mathbb{Z})$. De este modo, el producto de dos elementos de orden finito en el grupo G, no son necesariamente elementos de un grupo finito. ¿Y cómo es la cosa en un grupo abeliano?

5. Demostrar, que el grupo G de orden par $|G| = 2n$ necesariamente contiene un elemento $g \neq e$ de orden 2. (*Indicación*. Considerar la partición de G en pares g, g^{-1}).

6. Demostrar, que $S_n = \langle (12), (13), \ldots, (1n) \rangle$.

7. Demostrar, que $S_n = \langle (12), (123, \ldots, n) \rangle$.

8. Demostrar, que el grupo alternado A_n, $n \geqslant 3$, es engendrado por ciclos de longitud 3, además, efectivamente,

$$A_n = \langle (123), (124), \ldots, (12n) \rangle.$$

9. Hallar el signo de la permutación

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ n & n-1 & n-2 & \ldots & 2 & 1 \end{pmatrix}.$$

10. Sea $\Omega = \{1, 2, \ldots, n\}$, $\Omega \times \Omega$ un cuadrado cartesiano. Llamaremos al par $(i, j) \in \Omega \times \Omega$, *inversión en relación a la permutación* $\sigma \in S_n$ (brevemente: σ-*inversión*), si $i < j$, pero $\sigma(i) > \sigma(j)$. Hacemos

$$\operatorname{sgn} \sigma = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Como $(\sigma(j) - \sigma(i))/(j - i)$ es un número racional distinto de cero, siendo negativo exactamente cuando (i, j) es σ-inversión, y como $\sigma\colon \Omega \to \Omega$ es una aplicación biyectiva, entonces, $\operatorname{sgn} \sigma = (-1)^k$, donde k es el número general de las σ-inversiones. Si $\tau = (ij)$ es una trasposición, entonces, $\operatorname{sgn} \tau = -1$. Como es fácil ver,

$$(\sigma(j)\,\sigma(i))\,\sigma = \begin{pmatrix} \ldots \sigma(j) \ldots \sigma(i) \ldots \\ \ldots \sigma(i) \ldots \sigma(j) \ldots \end{pmatrix} \begin{pmatrix} \ldots i & \ldots j & \ldots \\ \ldots \sigma(i) & \ldots \sigma(j) & \ldots \end{pmatrix} =$$

$$= \begin{pmatrix} \ldots i & \ldots j & \ldots \\ \ldots \sigma(j) & \ldots \sigma(i) & \ldots \end{pmatrix},$$

así que la σ-inversión (i, j) deja de ser inversión en relación a la permutación $\tau\sigma$, donde $\tau = (\sigma(j)\,\sigma(i))$ es una trasposición. Mostrar, que se encuentran k trasposiciones $\tau_1, \ldots, \tau_k$, para las cuales $\tau_k \tau_{k-1} \ldots \tau_1 \sigma = e$, es una permutación unitaria. Por consiguiente, $\sigma = \tau_1 \ldots \tau_{k-1} \tau_k$, y $\operatorname{sgn} \sigma = (-1)^k = \varepsilon_\sigma$ son dos designaciones, con iguales atributos, de una misma invariante de permutación; sgn (del latín *signum*: signo). Hemos obtenido otra forma cómoda para determinar el signo de una permutación. Digamos, en relación a la permutación (4) que el conjunto de inversiones se compone de cinco pares (1, 5), (2,5), (3,5), (4,5), (6,7), así que $\operatorname{sgn} \pi = -1$. Prácticamente, la cuestión se reduce a calcular, en la fila inferior de la permutación π, la cantidad de números j, mayores que i, pero que se encuentran antes de i, para $i = 1, 2, \ldots, n - 1$.

11. Demostrar, que el subconjunto no vacío H del grupo (multiplicativo) finito G, es un subgrupo, si H es cerrado con relación a la multiplicación. Significa, en el caso dado, que la exigencia de que en H existan el elemento unidad e, y el inverso h^{-1} para cada $h \in H$, resulta superflua.

12. ¿Qué sistema de generadores se puede proponer para el grupo multiplicativo $(\mathbb{Q}_+, \cdot)$ de los números racionales positivos? (*Indicación*. Utilizar el teorema fundamental de la aritmética, del § 8 del cap. 1). ¿Existe o no en $(\mathbb{Q}_+, \cdot)$ un sistema de generadores finito?

13. Demostrar, que la k-ésima potencia π^k del ciclo $\pi = (12 \ldots n) \in S_n$ es el producto $d =$ m.c.d. (n, k) de los ciclos independientes, cada uno de los cuales tiene una longitud $q =$ m.c.m. $(n, d) = n/d$.

14. Sean $A, B \in M_n(\mathbb{R})$ y $(AB)^m = E$, para algún número entero m. ¿Es cierto, que $(BA)^m = E$?

§ 3. MORFISMOS DE LOS GRUPOS

1. Isomorfismos. Como ya se indicara antes, tres rotaciones φ_0, φ_1, φ_2, en sentido contrario a las agujas del reloj, en los ángulos de 0°, 120°, 240°, trasladan el triángulo equilátero P_3 sobre sí mismo.

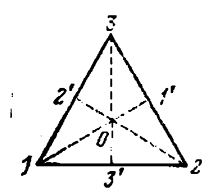


Fig. 13

Pero se tienen todavía tres *transformaciones axiales de simetría* (*de reflejo*) ψ_1, ψ_2, ψ_3 con los ejes de simetría 1— —1', 2— —2', 3— —3', indicados en la fig. 13. Todas las seis transformaciones de simetría corresponden a las permutaciones en el conjunto de los vértices del triángulo. Obtenemos

$$\varphi_0 \sim e, \quad \varphi_1 \sim (123), \quad \varphi_2 \sim (132)$$
$$\psi_1 \sim (23), \quad \psi_2 \sim (13), \quad \psi_3 \sim (12).$$

Como no hay otras permutaciones de potencia 3, entonces, se puede afirmar, que el grupo D_3 de todas las transformaciones de simetría del triángulo equilátero, manifiesta una gran similitud con el grupo simétrico S_3.

En este mismo sentido, son cercanos entre sí los grupos cíclicos C_n (véase el ejemplo en el punto 3 del § 2) y $\langle(12 \ldots n)\rangle \subset S_n$. Estos hechos, así como las meditaciones generales sobre grupos, no pueden no conducir a una pregunta natural, acerca de las propiedades más esenciales de los grupos. A primera vista, una información completa está contenida en la tabla de multiplicación del grupo G,

llamada *tabla de Cayley*

	g_1	g_2	$\cdots$	g_n	$\cdots$
g_1	g_1g_1	g_1g_2	$\cdots$	g_1g_n	$\cdots$
g_2	g_2g_1	g_2g_2	$\cdots$	g_2g_n	$\cdots$
$\cdot$					
$\cdot$					
$\cdot$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g_n	g_ng_1	g_ng_2	$\cdots$	g_ng_n	$\cdots$
$\cdot$					
$\cdot$					
$\cdot$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

Realmente, muchas regularidades de los grupos pueden ser percibidas al examinarse la tabla de Cayley, o, lo que es lo mismo, la matriz $M = (m_{ij})$ (de dimensiones $n \times n$, si $n = (G{:}e)$) con elementos $m_{ij} = g_ig_j \in G$. Sabemos, por ejemplo, que en cada fila y en cada columna de la matriz M, cualquier elemento del grupo G se encuentra exactamente una vez (véase más abajo, la demostración del teorema 2). El grupo G es abeliano si, y sólo si, la matriz M es simétrica, o sea, si $m_{ij} = m_{ji}$. Esta lista de propiedades se podría continuar, pero, sin embargo, comparar dos tablas para grupos G, G' de igual orden, es relativamente difícil, porque la forma de la matriz M depende de la numeración (ubicación) de los elementos del grupo, y ya en el caso de grupos infinitos, la situación se complica aún más.

El modo más correcto y más radical de abordar el problema de la diferenciación (o, por el contrario, de la identidad) de los grupos G y G', lo propone el concepto de isomorfismo.

DEFINICIÓN. Dos grupos G y G', con operaciones $*$ y $\circ$ se llaman *isomorfos*, si existe la aplicación $f\colon G \to G'$ tal, que:

(i) $f(a * b) = f(a) \circ f(b)$, *para todos los* $a, b \in G$;

(ii) f *es biyectiva*.

El hecho de isomorfismo de grupos, frecuentemente se designa con el símbolo $G \cong G'$.

Mencionemos las propiedades más sencillas del isomorfismo.

1) *La unidad pasa a unidad.* Efectivamente, si e es unidad en el grupo G, entonces, $e * a = a * e = a$, en consecuencia $f(e) \circ f(a) = f(a) \circ f(e) = f(a)$, de donde se deduce, que $f(e) = e'$, unidad del grupo G'. En este razonamiento fueron utilizados, aunque parcialmente, ambas propiedades de f. Para la (i) esto es evidente, y la propiedad (ii) garantiza la sobreyectividad de f, así que, con los elementos de $f(g)$, se completa todo el grupo G'. ■

2) $f(a^{-1}) = f(a)^{-1}$. Efectivamente, de acuerdo a 1), $f(a) \circ f(a^{-1}) = f(a * a^{-1}) = f(e) = e'$, que es unidad en G', de donde
$$f(a)^{-1} = f(a)^{-1} \circ e' = f(a)^{-1} \circ (f(a) \circ f(a^{-1})) =$$
$$= (f(a)^{-1} \circ f(a)) \circ f(a^{-1}) = e' \circ f(a^{-1}) = f(a^{-1}).$$ ■

3) *La aplicación inversa* $f^{-1}: G' \to G$ *(existente en virtud de la propiedad* (ii)), *también es isomorfismo.*

En razón del corolario del teorema 2, § 5, cap. 1, hay que convencerse solamente de la legitimidad de la propiedad (i) para f^{-1}. Sean, a', $b' \in G'$. Entonces, en vista de la biyectividad de f, tenemos $a' = f(a)$, $b' = f(b)$ para algunos a, $b \in G$. Por cuanto f es isomorfa, $a' \circ b' = f(a) \circ f(b) = f(a * b)$. De aquí, tenemos, $a * b = f^{-1}(a' \circ b')$, y como, a su vez, $a = f^{-1}(a')$, $b = f^{-1}(b')$, entonces, $f^{-1}(a' \circ b') = f^{-1}(a') * f^{-1}(b')$. ▌

Una sencilla comprobación muestra, que la relación $\sim$, establecida por nosotros entre los grupos D_3 y S_3, es realmente un isomorfismo.

En calidad de aplicación isomorfa f, del grupo multiplicativo $(\mathbb{R}_+, \cdot)$ de todos los números reales positivos sobre el grupo aditivo $(\mathbb{R}, +)$ de todos los números reales, puede servir $f = \ln$. La conocida propiedad del logaritmo $\ln ab = \ln a + \ln b$, precisamente modela la propiedad (i) en la definición de isomorfismo. Como inversa f, sirve la aplicación $x \mapsto e^x$.

Demostremos ahora dos teoremas generales, que ilustran sobre el papel del isomorfismo en la teoría de los grupos.

TEOREMA 1. *Todos los grupos cíclicos de un mismo orden (incluso, infinito) son isomorfos entre sí.*

DEMOSTRACION. Efectivamente, si $\langle g \rangle$ es un grupo cíclico infinito, entonces, todas las potencias g^n del generador g son distintas, y obtenemos el isomorfismo $f: \langle g \rangle \to (\mathbb{Z}, +)$, haciendo $g^n \mapsto f(g^n) = n$. La biyectividad de f es evidente, y la propiedad $f(g^m g^n) = f(g^n) + f(g^m)$, se deduce del teorema 2 del § 2.

Sean ahora, $G = \{e, g, \ldots, g^{q-1}\}$ y $G' = \{e', g', \ldots, (g')^{q-1}\}$ dos grupos cíclicos de orden q (no distinguimos las operaciones en G y G'). Definimos la aplicación biyectiva

$$f: g^k \mapsto (g')^k, \quad k = 0, 1, \ldots, q-1.$$

Haciendo, $n + m = lq + r$, $0 \leqslant r \leqslant q - 1$, para cualesquiera n, $m = 0, 1, \ldots, q - 1$ y razonando como al demostrar el teorema 3 del § 2, tendremos

$$f(g^{n+m}) = f(g^r) = (g')^r = (g')^{n+m} = (g')^n (g')^m = f(g^n) f(g^m). \quad ▌$$

TEOREMA 2 (de Cayley). *Cualquier grupo finito de orden* n, *es isomorfo a cierto subgrupo del grupo simétrico* S_n.

DEMOSTRACION. Sea G nuestro grupo, $n = |G|$. Se puede considerar, que S_n es el grupo de todas las aplicaciones biyectivas del conjunto G sobre sí mismo, debido a que la naturaleza de los elementos, permutados con los elementos de S_n, no es esencial.

Para cualquier elemento $a \in G$ examinamos la aplicación $L_a: G \to G$, definida por la fórmula

$$L_a(g) = ag.$$

Si $e = g_1, g_2, \ldots, g_n$, son todos los elementos del grupo G, entonces, $a, ag_2, \ldots, ag_n$, serán los mismos elementos, pero dispuestos en algún otro orden (¡recordemos la tabla de Cayley!). Esto es comprensible, por cuanto
$ag_i = ag_j \Rightarrow a^{-1}(ag_i) = a^{-1}(ag_j) \Rightarrow (a^{-1}a)\, g_i = (a^{-1}a)\, g_j \Rightarrow g_i = g_j$.
Esto significa, que L_a es una aplicación (permutación) biyectiva, cuya inversa será $L_a^{-1} = L_{a^{-1}}$. La aplicación unidad es, naturalmente, L_e.

Utilizando de nuevo la asociatividad de la multiplicación en G, obtenemos $L_{ab}(g) = (ab)\, g = a\,(bg) = L_a(L_b g)$, o sea, $L_{ab} = L_a \circ L_b$.

Así, el conjunto $L_e, L_{g_2}, \ldots, L_{g_n}$ genera un subgrupo, digamos H, en el grupo $S(G)$ de todas las aplicaciones biyectivas del conjunto G sobre sí mismo, o sea, en S_n. Tenemos la inclusión $H \subset S_n$ y tenemos la relación L: $a \mapsto L_a \in H$, que posee, por lo dicho antes, todas las propiedades de isomorfismo. ∎

El teorema de Cayley, no obstante a su sencillez, tiene gran importancia en la teoría de grupos. El destaca un cierto objeto universal (la familia $\{S_n \mid n = 1, 2, \ldots\}$ de grupos simétricos), que es contenedor de todos los grupos finitos en general, considerados con exactitud hasta el isomorfismo. La frase « con exactitud hasta el isomorfismo » no sólo refleja la esencia de la teoría de grupos, que pretende reunir en una clase a todos los grupos isomorfos, sino y de las matemáticas en su conjunto, las que, sin tales generalizaciones, carecerían de sentido.

Haciendo $G' = G$ en la definición de isomorfismo, obtenemos la aplicación isomorfa φ: $G \to G$ del grupo G sobre sí mismo. Ella se llama *automorfismo* del grupo G. Por ejemplo, la aplicación unitaria e_G: $g \mapsto g$ (más adelante indicada por medio del 1), es un automorfismo, pero, como regla, G posee también automorfismo no trivial. La propiedad 3) de las aplicaciones automorfas muestra, que la aplicación inversa en relación a un automorfimso, también será un automorfismo. Si, luego, φ, ψ son automorfismos del grupo G, entonces, $(\varphi \circ \psi)(ab) = \varphi(\psi(ab)) = \varphi(\psi(a)\, \psi(b)) = (\varphi \circ \psi)(a) \times (\varphi \circ \psi)(b)$ para cualesquiera $a, b \in G$. Por consiguionte, el conjunto Aut (G) de todos los automorfismos del grupo G genera el grupo—subgrupo del grupo $S(G)$ de todas las aplicaciones biyectivas $G \to G$.

2. Homomorfismos. En el grupo de automorfismos Aut (G) del grupo G hay un subgrupo especial. El se designa con el símbolo Inn (G) y se llama *grupo de automorfismos internos.* Sus elementos son aplicaciones

$$I_a : g \mapsto aga^{-1}.$$

Un pequeño ejercicio muestra que I_a efectivamente cumple todas las propiedades, que se requieren de los automorfismos, además

$I_a^{-1} = I_{a^{-1}}$, $I_e = 1$ es el automorfismo unidad,

$I_a \circ I_b = I_{ab}$ (porque $(I_a \circ I_b)(g) = I_a(I_b(g)) =$

$= I_a(bgb^{-1}) = abgb^{-1}a^{-1} = abg(ab)^{-1} = I_{ab}(g))$.

La última relación muestra, que la aplicación

$$f : G \to \mathrm{Inn}\,(G)$$

del grupo G' sobre el grupo Inn (G), de sus automorfismos internos, determinada por la fórmula $f(a) = I_a$, $a \in G$, posee la propiedad (i) de la aplicación isomorfa: $f(a) \circ f(b) = f(ab)$. Sin embargo, la propiedad (ii), en este caso, no se cumple necesariamente. Si, por ejemplo, G es un grupo abeliano, entonces, $aga^{-1} = g$ para todas las $a, g \in G$, así que $I_a = I_e$, y todo el grupo Inn (G) está compuesto de un solo elemento unidad I_e. Esta circunstancia hace natural la siguiente general

DEFINICION. La aplicación f: $G \to G'$ del grupo $(G, *)$ en $(G', \circ)$, se llama *homomorfismo* si

$$f(a * b) = f(a) \circ f(b),\ \forall a,\ b \in G$$

(en otras palabras, en la definición de isomorfismo se suprime la propiedad (ii)).

Se llama *núcleo* del homomorfismo f el conjunto

$$\mathrm{Ker}\, f = \{g \in G \mid f(g) = e',\ \text{unidad del grupo } G'\}.$$

La aplicación homomorfa de un grupo sobre sí mismo, también se llama *endomorfismo.*

En esta definición, de f no sólo no se exige biyectividad, sino que tampoco se requiere sobreyectividad (o sea, ser aplicación « sobre »), lo que por otra parte, no es muy esencial, puesto que siempre se puede uno limitar al examen de la imagen $\mathrm{Im}\, f \subset G'$, que es, evidentemente, subgrupo en G'. La principal distinción del homomorfismo de f con respecto al isomorfismo, se reduce a la existencia de un núcleo no trivial Ker f, que es, por así decirlo, la medida de la no inyectividad de f. Pero si, Ker $f = \{e\}$, entonces f: $G \to \mathrm{Im}\, f$, es isomorfismo.

Notemos, que

$$f(a) = e',\ f(b) = e' \Rightarrow f(a * b) = f(a) \circ f(b) = e' \circ e' = e'$$

y

$$f(a^{-1}) = f(a)^{-1} = (e')^{-1} = e'.$$

Por eso, el núcleo Ker f es subgrupo en G. Sea $H = \mathrm{Ker}\, f \subset G$. Entonces (ahora omitimos los signos $*$ y $\circ$):

$$f(ghg^{-1}) = f(g)\, f(h)\, f(g)^{-1} = f(g)\, e' f(g)^{-1} = e',$$

$$\forall h \in H,\ g \in G,$$

o sea, $ghg^{-1} \in H$ y, por consiguiente, $gHg^{-1}H$. Reemplazando aquí g por g^{-1}, obtenemos $g^{-1}Hg \subset H$, de donde $H \subset gHg^{-1}$. Así que,

$$gHg^{-1} = H, \quad \forall g \in G.$$

Los subgrupos que tienen estas propiedades se llaman normales (también los llaman subgrupos invariantes, o divisores normales). Así, hemos demostrado el

TEOREMA 3. *Los núcleos de los homomorfismos siempre son subgrupos normales.* $\blacksquare$

La importancia de este hecho la evaluaremos en la medida necesaria considerablemente más tarde. Por ahora apuntemos, que no todo subgrupo es normal en G. Por ejemplo, en S_3 el subgrupo cíclico $\langle(123)\rangle = A_3$, es normal, pero $\langle(12)\rangle = \{e, (12)\}$ no lo es tal (no se recomienda llamar a $\langle(12)\rangle$ «subgrupo no normal»).

3. Vocabulario. Ejemplos. Cabe anotar, que los términos «aplicación sobreyectiva» (aplicación «sobre»), inyectiva (aplicación de inclusión), biyectiva (aplicación biunívoca), empleados para las aplicaciones de cualesquiera conjuntos (sin operaciones), en el caso de los grupos (y en el caso de otros sistemas algebraicos) son reemplazados por los términos correspondientes de *epimorfismo* (homomorfismo «sobre»), *monomorfismo* (homomorfismo con núcleo unitario), *isomorfismo* (homomorfismo biunívoco, epimorfismo y monomorfismo conjuntamente). Existe la tendencia a reemplazar homomorfismo por el término *morfismo*. Es útil tener en vista este vocabulario al leer literatura matemática, pero al principio, quienes lo deseen pueden arreglárselas con dos términos: isomorfismo y homomorfismo con el agregado de las partículas «sobre» y «en».

Como complemento de lo considerado arriba, damos algunos ejemplos más de morfismos de grupos.

1) El grupo aditivo de los números enteros $\mathbb{Z}$, homomórficamente se representa sobre el grupo cíclico finito $\langle g\rangle$ de orden q, si hacemos $f\colon n \mapsto g^n$ (véase el teorema 2 del § 2). En este caso, evidentemente, Ker f $\{lq \mid l \in \mathbb{Z}\}$. Efectivamente, es claro que $\{lq\} \subset \operatorname{Ker} f$. La inclusión inversa se deduce del teorema 3 del § 2.

2) La aplicación $f\colon \mathbb{R} \to T = SO(2)$ del grupo aditivo de los números reales sobre el grupo T de rotaciones del plano con un punto fijo 0, dada por la fórmula $f(\lambda) = \Phi_\lambda$ (Φ_λ es rotación en sentido contrario a las agujas del reloj, en el ángulo $2\pi\lambda$), es homomorfa. Como $\Phi_\lambda \circ \Phi_\mu = \Phi_{\lambda+\mu}$, y el giro en un ángulo múltiplo de 2π, coincide con el giro unitario (en un ángulo nulo), entonces, $\operatorname{Ker} f = \{2\pi n \mid n \in \mathbb{Z}\}$. Se dice también, que f es un homomorfismo de $\mathbb{R}$ en la circunferencia S^1 de radio unitario, por cuanto se tiene correspondencia biunívoca entre Φ_λ y el punto en S^1 con coordenadas polares $(1, 2\pi\lambda)$, $0 \leqslant \lambda < 1$.

3) El grupo lineal completo $GL(n)$ de las matrices reales A ((o sea, de las matrices con coeficientes en $\mathbb{R}$) con determinantes $\det A$ distintos de cero, homomórficamente se representa sobre el grupo multiplicativo $\mathbb{R}^*$. de los números reales distintos de cero, si se hace $f = \det$. La condición de homomorfismo $f(AB) = f(A)f(B)$ es sólo otra formulación distinta del teorema 5 del § 2 del cap. 3. Por definición, $SL(n) = \operatorname{Ker} f$.

4) Consideremos el grupo cíclico $C_2 = \langle -1 \rangle = \{1, -1\}$ de orden 2. Si se quiere, se puede dar en forma abstracta como una tabla de Cayley

$$C_2: \quad \begin{array}{c|cc} \cdot & 1 & -1 \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \end{array}$$

La aplicación $S_n \to C_2$ con ayuda de nuestra conocida función $\varepsilon = \mathrm{sgn} : \pi \mapsto \varepsilon_\pi$ (el signo de la permutación π) es un homomorfismo del grupo simétrico S_n sobre C_2. Además, de acuerdo a la definición de grupo alternado, Ker $\varepsilon = A_n$.

5) Un grupo infinito puede ser isomorfo de su verdadero (propio) subgrupo. Efectivamente, el grupo aditivo $(\mathbb{Z}, +)$ contiene al subgrupo propio $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, donde $n > 1$ es un número natural dado. Es fácil verificar que la aplicación $g_n : \mathbb{Z} \to n\mathbb{Z}$, está determinada por la relación $g_n(k) = nk$ es un isomorfismo. De paso notemos, que $\mathbb{Z}$ y $n\mathbb{Z}$, son grupos cíclicos infinitos, en los cuales de generador sirven 1 o -1 y n o $-n$, respectivamente; por eso, g_n y la aplicación $k \mapsto -nk$ agotan todos los isomorfismos de $\mathbb{Z} \to n\mathbb{Z}$.

6) El grupo Aut (G) e incluso un elemento no unitario $\varphi \in$ Aut (G) aislado, pueden servir de fuente de importantes informaciones sobre el grupo G. He aquí un ejemplo claro de este tipo. Sea G un grupo finito, en el cual opera un automorfismo de orden 2 ($\varphi^2 = 1$), sin puntos fijos:

$$a \neq e \Rightarrow \varphi(a) \neq a.$$

Presupongamos, que $\varphi(a)\, a^{-1} = \varphi(b)\, b^{-1}$ para algunos $a, b \in G$. Entonces, luego de multiplicar a esta igualdad a la izquierda por $\varphi(b)^{-1}$ y a la derecha por a, obtenemos $\varphi(b)^{-1}\varphi(a) = b^{-1}a$, o sea $\varphi(b^{-1}a) = b^{-1}a$, de donde $b^{-1}a = e$ y $b = a$. Así, $\varphi(a)\, a^{-1}$ hace el recorrido, junto con a, de todos los elementos del grupo G, o, lo que es equivalente, cualquier elemento $g \in G$ se escribe de la forma $g = \varphi(a)\, a^{-1}$. Pero en tal caso, $\varphi(g) = \varphi(\varphi(a))\, \varphi(a^{-1}) = \varphi^2(a)\, \varphi(a^{-1}) = a\varphi(a)^{-1} = (\varphi(a)\, a^{-1})^{-1} = g^{-1}$. De suerte que φ coincide con la aplicación $g \mapsto g^{-1}$. Sabiendo esto, obtenemos $ab = \varphi(a^{-1})\ \varphi(b^{-1}) = \varphi(a^{-1}b^{-1}) = (a^{-1}b^{-1})^{-1} = ba$, o sea, ¡el grupo G resulta ser abeliano! Además, $(G : e)$ es un número impar, porque G se compone de e y de pares de elementos no intersecados g_i, $g_i^{-1} = \varphi(g_i)$.

7) En cuanto se puede modificar una operación sobre un grupo, no cambiando, en el sentido del isomorfismo, el propio grupo, lo muestra el siguiente ejemplo (véase también el ejercicio 3 del § 1). Sean, G un grupo arbitrario, t un elemento suyo dado, cualquiera. Introducimos en el conjunto G una nueva operación:

$$(g, h) \mapsto g * h = gth.$$

Inmediatamente comprueba, que $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$, o sea, que la operación $*$ es asociativa. Además, $g * t^{-1} = t^{-1} * g = g$, y $g * (t^{-1}g^{-1}t^{-1}) = (t^{-1}g^{-1}t^{-1}) * g = t^{-1}$, y esto significa, que $(G, *)$ es un grupo con elemento unidad $e_* = t^{-1}$. De elemento inverso a g en $(G, *)$, sirve $g_*^{-1} = t^{-1}g^{-1}t^{-1}$. La aplicación $f: g \mapsto gt^{-1}$, establece el isomorfismo de los grupos $(G, \cdot)$ y $(G, *)$, o sea, $f(gh) = f(g) * f(h)$.

Todos los ejemplos indicados sirven, entre otras cosas, para ilustrar una regla común: el estudio de los morfismos del grupo G da una considerable información sobre el mismo grupo G.

4. Clases adjuntas respecto a un subgrupo. De la definición de homomorfismo $f: G \to G'$ y de los ejemplos considerados se ve, que

todos los elementos del conjunto

$$a \operatorname{Ker} f = \{ab \mid b \in \operatorname{Ker} f\}, \quad a \in G,$$

tienen aplicación en un mismo elemento $f(a)$ del grupo G': $f(ab) = f(a) f(b) = f(a) e' = f(a)$. Por el contrario, si $f(g) = f(a)$, entonces, $f(a^{-1}g) = f(a^{-1}) f(g) = f(a)^{-1} f(g) = e'$, de donde $a^{-1}g = b \in \operatorname{Ker} f$ y $g = ab \in \operatorname{Ker} f$. Este hecho, muestra la conveniencia de descomponer al G en subconjuntos del tipo $a \operatorname{Ker} f$. Estudiemos esta subdivisión en el caso general, independientemente de los homomorfismos.

DEFINICION. Sea H un subgrupo del grupo G. *Clase adjunta a la izquierda en el grupo G del subgrupo H* (brevemente, G del H) se llama el conjunto gH de elementos del tipo gh, donde g es un elemento dado de G, y h recorre todos los elementos del subgrupo H. El elemento g se denomina *representante* de la clase adjunta gH.

Análogamente se definen las *clases Hg adjuntas a la derecha*. A veces, las clases adjuntas a la izquierda en nuestro sentido, las llaman a la derecha, y a las adjuntas a la derecha, a la izquierda. Lo importante es atenerse a una terminología dada. Si $H = \operatorname{Ker} f$ es el núcleo de un homomorfimo, entonces, $gH = Hg$, en vista de la normalidad de H en G (véase el punto 2). Hagamos notar, que una de las clases adjuntas, resulta ser el propio subgrupo $H = He = eH$. Ninguna otra clase adjunta es subgrupo. Efectivamente, si gH es un subgrupo, entonces, $e \in gH$, de donde $e = gh$, $g = h^{-1}$ y $gH = h^{-1}H = H$.

TEOREMA 4. *Dos clases adjuntas a la izquierda en G del H, o coinciden, o no tienen ningún elemento común. La descomposición de G en clases adjuntas a la izquiedra de H, define en G la relación de equivalencia.*

DEMOSTRACION. Sea que las clases g_1H y g_2H tienen un elemento común $a = g_1h_1 = g_2h_2$. Entonces $g_2 = g_1h_1h_2^{-1}$, y cualquier elemento g_2h de la clase g_2H tiene la forma $g_1h_1h_2^{-1}h = g_1h'$, donde $h' = h_1h_2^{-1}h \in H$. Quiere decir, que $g_2H \subset g_1H$. Análogamente se demuestra, que todo elemento de la clase g_1H, está contenido en g_2H, y, por consiguiente, $g_1H = g_2H$.

Como todo elemento, dado de antemano, $g \in G$, está contenido en gH, entonces, el razonamiento efectuado demuestra, que G se presenta en forma de unión de las clases adjuntas a la izquierda disjuntas respecto al subgrupo H;

$$G = \bigcup g_i H.$$

De acuerdo al principio general, expuesto en el § 6 del cap. 1, esta descomposición induce en G la relación de equivalencia, la que se define de modo evidente:

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

Si se desea, de la reflexividad, simetría y transitividad de esta relación, se puede uno convencer inmediatamente: $a \sim a$, por cuanto $a^{-1}a = e \in H$; $a \sim b \Leftrightarrow a^{-1}b = h \Leftrightarrow b^{-1}a = h^{-1} \in H \Leftrightarrow b \sim a$; $a \sim \sim b$, $b \sim c \Rightarrow b^{-1}a = h_1$, $c^{-1}b = h_2 \Rightarrow c^{-1}a = c^{-1}bh_1 = h_2h_1 \in \in H \Rightarrow a \sim c$. ∎

Una afirmación análoga tiene lugar para las clases adjuntas a la derecha.

La descomposición en clases adjuntas surge de un modo natural en los grupos de permutaciones. Sea, por ejemplo, $G = S_n$, un grupo simétrico, operando en el conjunto $\Omega = \{1, 2, \ldots, n\}$. Si se examina la agrupación de H elementos $\pi \in S_n$, tales que $\pi(n) = n$, entonces, como es fácil convencerse, H es un subgrupo en S_n, que se puede identificar con S_{n-1}. Sean, $\tau_0 = e$, $\tau_i = (in)$, trasposiciones, que transforman a n en i ($i = 1, 2, \ldots, n - 1$), Es claro, que

$$S_n = \bigcup_{k=0}^{n-1} \tau_k S_{n-1}.$$

Examinemos la descomposición S_3 en clases adjuntas a la izquierda y derecha, del subgrupo $\langle(12)\rangle = S_2$:

$$S_3 = \{e, (12)\} \cup \{(13), (123)\} \cup \{(23), (132)\};$$
$$S_3 = \{e, (12)\} \cup \{(13), (132)\} \cup \{(23), (123)\}.$$

Vemos, que el conjunto de las clases adjuntas a la izquierda gS_2, no coincide con el conjunto de las clase adjuntas a la derecha S_2g'. No obstante, entre los conjuntos $\{gH\}$ y $\{Hg'\}$ siempre se tiene una correspondencia biyectiva, por la cual

$$x = gh \in gH \leftrightarrow x^{-1} = h^{-1}g^{-1} \in Hg^{-1}.$$

Efectivamente, si, por ejemplo, $h_1g_1^{-1} = h_2g_2^{-1}$, entonces, $g_1 = = g_2h_2^{-1}h_1$ y $g_1H = g_2H$. En particular, *si $\{e, x, y, z, \ldots\}$ es un conjunto de representantes de clases simétricas a la izquierda (correspondientemente, a la derecha), entonces, $\{e, x^{-1}, y^{-1}, z^{-1}, \ldots\}$ es el conjunto de representantes de clases adjuntas a la derecha (correspondientemente, a la izquierda). Las potencias de estos conjuntos, coinciden.* ∎

Al conjunto de todas las clases adjuntas a la izquierda en G de H, acordamos designarlo con el símbolo G/H (o $(G/H)_l$, si surge la necesidad de examinar a un mismo tiempo el conjunto $(G/H)_r$ de clases adjuntas a la derecha en G de H). Para la potencia Card G/H de este conjunto, se usa el nombre de «*índice de subgrupo H en G*» y se introduce la designación especial $(G: H)$, que concuerda muy bien con la designación $(G : e)$ de orden $|G|$ del grupo G (el número de clases adjuntas del grupo unidad). Como la aplicación $H \rightarrow gH$ es biunívoca (recuerde la demostración del teorema de Cayley y la aplicación L_g), entonces, Card $gH = (H : e)$. De este modo, tiene

lugar la fácilmente memorizable fórmula

$$(G : e) = (G : H)\,(H : e),$$

de la cual se deduce el clásico

TEOREMA 5 (de Lagrange). *El orden de un grupo finito es divisible por el orden de cada uno de sus subgrupos.* ∎

COROLARIO. *El orden de cualquier elemento es un divisor del orden del grupo. Un grupo de orden primo p, es siempre cíclico y, con exactitud hasta el isomorfismo, único.*

Efectivamente, el orden de cualquier elemento $g \in G$ coincide con el orden del subgrupo cíclico engendrado por él $\langle g\rangle$ (teorema 3 del § 2). Si, luego, $|G| = p$ es un número primo, y H un grupo no unitario, entonces, la divisibilidad de p por $|H|$ significa, que $|H| = p$, de donde, $H = G$. Por consiguiente G coincide con el subgrupo cíclico, engendrado por cualquier elemento $g \neq e$. Todos los grupos cíclicos del orden dado, son isomorfos (teorema 1). Esto da derecho a habla de la unicidad. ∎

En relación con el teorema de Lagrange, surge la tentación de buscar, para cada divisor de m de orden n del grupo G, un subgrupo de orden m en G. Pero para esto, en general, no hay fundamento. Quienes lo deseen pueden comprobar, que en el grupo alterno A_4, de orden 12, no hay subgrupos de orden 6.

Pero en algunos grupos la «invocación del teorema de Lagrange» es correcta. Por ejemplo, tiene lugar el

TEOREMA 6. *Todo subgrupo de un grupo cíclico, es a su vez un grupo cíclico. Los subgrupos del grupo cíclico infinito $(\mathbb{Z}, +)$ se agotan con los grupos (infinitos) $(m\mathbb{Z}, +)$, $m \in \mathbb{N}$, y los subgrupos del grupo cíclico de orden q, se hallan en correspondencia biunívoca con los divisores (positivos) d del número q.*

DEMOSTRACION. Para diferenciar, examinaremos el grupo cíclico $A = \langle a\rangle$ en escritura aditiva. Cada uno de sus elementos, por consiguiente, tiene la forma ka, donde $k \in \mathbb{Z}$ o $k = 0, 1, \ldots, q - 1$, si A es un grupo finito de orden q (véase el teorema 3 del § 2). Sea B, una matriz no nula en A. Si $ka \in B$ para algún $k \neq 0$, entonces, también $-ka \in B$. Entre todos los elementos $ka \in B$ con k positivo, eligimos el elemento ma, donde m es el menor.

Escribiendo cualquier $k > 0$ en forma de $k = lm + r$, $0 \leqslant r < m$, vemos, que de $ka \in B$ sigue $ra = ka - l\,(ma) \in B$, o sea, $r = 0$. Quiere decir, $B = \langle ma\rangle$, es un grupo cíclico.

Todos los grupos cíclicos infinitos son isomorfos (teorema 1). Tomemos en calidad de modelo al grupo aditivo $(\mathbb{Z}, +)$. En el caso dado, sirven de generadores 1 o -1, así que, por lo demostrado, cualquier subgrupo en $(\mathbb{Z}, +)$ es definido por el número natural

m y tiene la forma

$$m\mathbb{Z} = \langle m \cdot 1 \rangle = \{0, \pm m, \pm 2m, \ldots\}.$$

Evidentemente, todos estos subgrupos son infinitos.

Sean ahora, $\langle a \rangle = \langle 0, a, \ldots, (q-1)\,a \rangle$, $qa = 0$. Sabemos, que $B = \langle 0, ma, 2ma, \ldots \rangle$, donde $m \in \mathbb{N}$, además $sa \in B$, $s \in \mathbb{N} \Rightarrow$ $\Rightarrow s = mt$. Se afirma, que m divide a q. Efectivamente sea $q =$ $= dm + r$, $0 \leqslant r < m$. Entonces

$$0 = qa = d\,(ma) + ra,$$

de donde, $ra = -d\,(ma) \in B$. El ser m un mínimo, conlleva a $r = 0$ y tenemos $q = dm$. De este modo,

$$B = \{0, ma, 2ma, \ldots, (d-1)\,ma\} = mA$$

es un subgrupo en A de orden d. Cuando m hace el recorrido por todos los divisores positivos del número q, lo mismo hace d, y obtenemos exactamente sólo un subgrupo por cada orden d, divisor de q. ∎

COROLARIO *En el grupo cíclico $\langle a \rangle$ de orden q, el subgrupo de orden $d \mid q$ coincide con el conjunto de los elementos $b \in \langle a \rangle$ tales, que $db = 0$.*

DEMOSTRACION. Si $dm = q$, entonces, $b \in B = mA$ y $db = 0$. Por el contrario, sean, $b = la \in \langle a \rangle$ y $db = 0$. De la condición $dla = 0$, sigue, que $dl = qk = dmk$, de donde, $l = mk$ y $b = la = k\,(ma) \in$ $\in mA$. ∎

5. Monomorfismo $S_n \to GL\,(n)$. Recordemos, que se llama monomorfismo de los grupos $G \to G'$, a la inclusión isomorfa de G en G'.

TEOREMA 7. *Existe un monomorfismo $f\colon S_n \to GL\,(n)$ tal, que la matriz $f\,(\pi)$, $\pi \in S_n$, tiene determinante $|\,f\,(\pi)\,| = \varepsilon_\pi$.*

DEMOSTRACION. A cualquier matriz (a_{ij}) de dimensiones $n \times n$, la escribimos en forma de unión de columnas: $(a_{ij}) = (A^{(1)}, A^{(2)}, \ldots$ $\ldots, A^{(n)})$. Sean, en particular,

$$E^{(1)} = \begin{Vmatrix} 1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{Vmatrix}, \quad E^{(2)} = \begin{Vmatrix} 0 \\ 1 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{Vmatrix}, \quad \ldots, \quad E^{(n)} \begin{Vmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 1 \end{Vmatrix}$$

columnas de la matriz unidad E. Definimos la aplicación $f\colon S_n \to$ $\to GL\,(n)$, haciendo

$$\pi \mapsto f\,(\pi) = (E^{(\pi(1))}, E^{(\pi(2))}, \ldots, E^{(\pi(n))}). \qquad (1)$$

De este modo, $f\,(\pi)$ es una $n \times n$-matriz, en la que en cada una de sus filas y en cada una de sus columnas, hay exactamente una unidad y los demás lugares están ocupados por ceros. Es fácil comprender, que $f\,(\pi) \in GL\,(n)$.

Sean σ, π dos permutaciones arbitrarias, $\pi = \sigma\tau$ el producto de las mismas. Por definición, en la i-ésima fila de la matriz $f(\sigma) = (a_{is})$ y en la j-ésima columna de la matriz $f(\tau) = (b_{kl})$, los elementos distintos de cero serán, respectivamente, $a_{i\sigma^{-1}(i)} = 1$ y $b_{\tau(j),j} = 1$. Por eso, para la matriz $f(\sigma) f(\tau) = (c_{ij})$, la condición $c_{i,j} \neq 0$, es equivalente a $\sigma^{-1}(i) = \tau(j)$, o sea a $i = \sigma\tau(j) = \pi(j)$, y esto, precisamente, significa, que $f(\sigma) f(\tau) = f(\sigma\tau)$. En consecuencia, f es un homomorfismo.

La propiedad $\operatorname{Ker} f = e$ es evidente, por cuanto, inmediatamente de (1) se ve, que $f(\pi) = E \Rightarrow \pi = e$. Por consiguiente, f es un monomorfismo.

Finalmente, sabemos que el determinante es función antisimétrica de sus columnas. Por eso, $|f(\pi)| = g(E^{(1)}, \ldots, E^{(n)})$ es función antisimétrica de los argumentos $E^{(1)}, \ldots, E^{(n)}$. De (1), las definiciones de las operaciones S_n sobre g (véase (5) del § 2) y de la demostración del teorema 5 del § 2, percibimos, que

$$\begin{aligned}\varepsilon_\pi |f(\pi)| = \varepsilon_\pi \cdot g(E^{(1)}, \ldots, E^{(n)}) = (\pi \circ g)(E^{(1)}, \ldots, E^{(n)}) =\\ = g(E^{(\pi^{-1}(1))}, \ldots, E^{(\pi^{-1}(n))}) = |E^{(1)}, \ldots, E^{(n)}| =\\ = \det E = 1. \text{ Así que, } |f(\pi)| = \varepsilon_\pi. \blacksquare\end{aligned}$$

Las matrices del tipo $f(\pi)$, $\pi \in S_n$, se llaman *matrices de permutaciones*. Una limitación del monomorfismo f sobre A_n, es el monomorfismo en $SL(n, \mathfrak{R})$. La composición $f \circ L$ de las aplicaciones $L: G \to S_n$ (teorema 2) y $f: S_n \to GL(n)$, lleva al monomorfismo $G \to GL(n)$ de cualquier grupo finito G. En el caso de S_3, la aplicación f tiene el siguiente aspecto:

$$e \mapsto \begin{Vmatrix}1&0&0\\0&1&0\\0&0&1\end{Vmatrix}, \quad (12) \mapsto \begin{Vmatrix}0&1&0\\1&0&0\\0&0&1\end{Vmatrix}, \quad (13) \mapsto \begin{Vmatrix}0&0&1\\0&1&0\\1&0&0\end{Vmatrix},$$

$$(23) \mapsto \begin{Vmatrix}1&0&0\\0&0&1\\0&1&0\end{Vmatrix}, \quad (123) \mapsto \begin{Vmatrix}0&0&1\\1&0&0\\0&1&0\end{Vmatrix}, \quad (132) \mapsto \begin{Vmatrix}0&1&0\\0&0&1\\1&0&0\end{Vmatrix}.$$

Con ayuda del teorema 7, se demuestra fácilmente **el llamado** ***teorema sobre el desarrollo completo de un determinante.***

TEOREMA 8. *El determinante*

$$\det A = \begin{vmatrix}a_{11} & a_{12} & \ldots & a_{1n}\\ a_{21} & a_{22} & \ldots & a_{2n}\\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn}\end{vmatrix}$$

se puede escribir en forma de una suma algebraica de n! productos (denominados términos del determinante):

$$\det A = \sum_{\pi \in S_n} \varepsilon_\pi a_{\pi(1),\,1} a_{\pi(2),\,2} \ldots a_{\pi(n),\,n}. \tag{2}$$

DEMOSTRACION. Designamos por medio de $|A^{(1)}, \ldots, A^{(j-1)}, E^{(i)}, A^{(j+1)}, \ldots, A^{(n)}|$ al determinante, que se obtiene de $|A|$ cambiando la columna $A^{(j)}$ con el número j, por la columna $E^{(i)}$ de la matriz unidad. La fórmula para desarrollar un determinante por los elementos de su j-ésima columna muestra, que para el complemento algebraico A_{ij} del elemento a_{ij} del determinante $|A| = |A^{(1)}, \ldots, A^{(n)}|$, se tiene, en forma de determinante de orden n, la expresión:

$$A_{ij} = |A^{(1)}, \ldots, A^{(j-1)}, E^{(i)}, A^{(j+1)}, \ldots, A^{(n)}|,$$

de donde, por la misma fórmula, se obtiene,

$$\det A = \sum_i a_{ij} A_{ij} = \sum_i a_{ij} |A^{(1)}, \ldots, A^{(j-1)}, E^{(i)}, A^{(j+1)}, \ldots, A^{(n)}|.$$

Si aplicamos esto al principio para $j = 1$, y luego (a cada uno de los n sumandos) para $j = 2$, etc., entonces, para $\det A$ tendremos expresiones contenedoras, respectivamente, de n, n^2, y, finalmente, n^n determinantes

$$\begin{aligned}\det A &= \sum_{i_1} a_{i_1,\,1} |E^{(i_1)}, A^{(2)}, \ldots, A^{(n)}| = \\ &= \sum_{i_1} a_{i_1,\,1} \sum_{i_2} a_{i_2,\,2} |E^{(i_1)}, E^{(i_2)}, A^{(3)}, \ldots, A^{(n)}| = \\ &= \sum_{i_1,\,i_2} a_{i_1,\,1} a_{i_2,\,2} |E^{(i_1)}, E^{(i_2)}, \ldots, A^{(n)}| = \ldots \\ &\ldots = \sum_{i_1,\,i_2,\,i_n} a_{i_1,\,1} a_{i_2,\,2} \ldots a_{i_n,\,n} |E^{(i_1)}, E^{(i_2)}, \ldots, E^{(i_n)}|.\end{aligned}$$

Aquí, $i_1, i_2, \ldots, i_n$, recorren cualquier surtido de los números $1, 2, \ldots, n$, (incluso con repeticiones). Utilizando todas las n^n aplicaciones distintas $\pi\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ (véase el ejemplo 1) del punto 2 del § 1), donde $\pi(1) = i_1, \ldots, \pi(n) = i_n$, escribimos de nuevo la expresión para $\det A$ de la forma

$$\det A = \sum_\pi a_{\pi(1),\,1} a_{\pi(2),\,2} \ldots a_{\pi(n),\,n} |E^{(\pi(1))}, E^{(\pi(2))}, \ldots, E^{(\pi(n))}|$$

(la suma comprende todos los π). Queda por indicar que, si $\pi(i) = \pi(j)$ para dos cualesquiera índices i y j distintos, entonces, en el determinante $|E^{(\pi(1))}, \ldots, E^{(\pi(n))}|$ dos columnas coinciden y, en consecuencia, es nulo. Por consiguiente, el determinante $|E^{(\pi(1))}, \ldots, E^{(\pi(n))}|$ sólo es distinto de cero, cuando la aplicación π es biunívoca, o sea, cuando es permutación. Pero en ese caso,

por el teorema 7, tenemos $|E^{(\pi(1))}, \ldots, E^{(\pi(n))}| = |f(\pi)| = \varepsilon_\pi$. ■

Observación. Por supuesto, al teorema 8 no es difícil demostrarlo por inducción directamente sobre n, sin ninguna mención de los grupos, aunque los signos ε_π delante de los términos del determinante tienen, en último análisis, una naturaleza teórica de grupo. El teorema 7, presenta un interés independiente.

Prestemos atención al hecho de que el teorema 8 se puede poner en la base de la teoría de determinantes (lo que frecuentemente se hace). Precisamente, dando el determinante del A por medio de la fórmula (2), nosotros hubiésemos obtenido todas sus propiedades, incluyendo la fórmula de desarrollo del det A por los elementos de la primera (o de la j-ésima) columna, que fue para nosotros, en el cap. 3, el punto de partida.

EJERCICIOS

1. Demostrar que, con exactitud hasta el isomorfismo, existe solamente un número finito $\rho(n)$ de grupos del orden dado n. (*Indicación.* Valorar en su

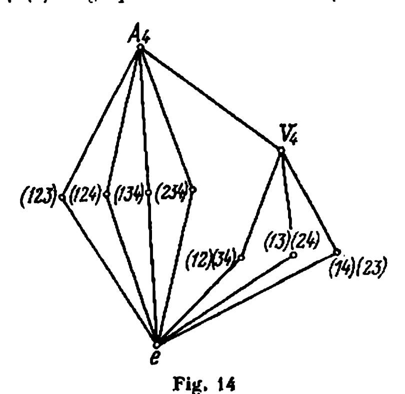


Fig. 14

parte superior el número de distintas tablas de Cayley de orden n. Los razonamientos formales con el uso del teorema 2, limitan a $\rho(n)$ al número $\binom{n!}{n}$ de distintos subconjuntos de n elementos, en S_n. Efectivamente, $\rho(n)$ es significativamente menor, pero una evaluación buena, cercana a la exacta, hasta ahora no ha sido hallada).

2. Utilizando el ejercicio 7 del § 2, mostrar, que cada grupo finito puede ser incluido (o sea, para él existe monomorfismo) en un grupo finito con dos generadores.

3. Demostrar, que en cualquier grupo, un subgrupo de índice 2, es necesariamente normal. (*Indicación.* Descomponer G por H, al principio en clases adjuntas a la izquierda, y luego adjuntas a la derecha, con los mismos representantes).

4. Con ayuda del ejercicio 3 pruebe de demostrar, que, con exactitud hasta el isomorfismo, S_3 es el único grupo no abeliano de orden 6.

5. Trate de convencerse de que en el diagrama (fig. 14), se hallan representados todos los subgrupos del grupo alternado A_4. Con el símbolo V_4 se designa

el llamado grupo *cuaternario* (o grupo de Klein) $V_4 = \{e, (12)(34), (13)(24), (14(23)\}$, y junto a los otros vértices del diagrama se han colorado los generadores de los subgrupos cíclicos.

6. Mostrar, que todos los grupos de orden 4 son abelianos y que con exactitud hasta el isomorfismo se completan con grupos de permutaciones $U = \langle(1234)\rangle$, V_4 o con grupos de matrices:

$$L_1 = \left\{ \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \begin{Vmatrix} 0 & 0 \\ -1 & 0 \end{Vmatrix}, \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix}, \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} \right\} \subset GL(2, \mathbb{R})$$

$$L_2 = \left\{ \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}, \begin{Vmatrix} -1 & 0 \\ 0 & 1 \end{Vmatrix}, \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix} \right\} \subset GL(2, \mathbb{R}).$$

Escribir en forma explícita los isomorfismos $U \to L_1$, $V_4 \to L_2$. (*Indicación.* Si $x^2 = e$ para cualquier elemento $x \in G$, entonces, $abab = e \Rightarrow ab = b^{-1}a^{-1} = b(b^{-1})(a^{-1})^2 a = beea = ba$.)

§ 4. ANILLOS Y CAMPOS

1. Definición y propiedades generales de los anillos. Las estructuras algebraicas $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$ ya aparecieron en calidad de primeros ejemplos de monoides, además consideramos a $(\mathbb{Z}, +)$ más tarde como un grupo abeliano aditivo (prácticamente cíclico). En la vida diaria, sin embargo, estas estructuras casi siempre se unen y se obtiene lo que en matemáticas se denomina anillo. Un elemento importante de la aritmética elemental se encierra en la ley distributiva (o combinatoria) $(a + b)c = ac + bc$, que parece trivial sólo debido a la costumbre adquirida. Intentando, por ejemplo, unir las estructuras algebraicas $(\mathbb{Z}, +)$, $(\mathbb{Z}, \circ)$, donde $n \circ m = n + m + nm$, nosotros ya no observaremos un acuerdo tan evidente entre dos operaciones binarias. Antes de pasar a futuros ejemplos, demos una definición exacta de anillo.

DEFINICION. Sea K un conjunto no vacío, en el cual son dadas dos operaciones (binarias algebraicas), $+$ (suma) y $\cdot$ (multiplicación), que cumplen las siguientes condiciones:

(K1) $(K, +)$ es un grupo abeliano;

(K2) $(K, \cdot)$ es un semigrupo;

(K3) las operaciones de suma y de multiplicación están vinculadas por medio de leyes distributivas (en otras palabras: la multiplicación es distributiva respecto a la suma):

$$(a + b)c = ac + bc, \quad c(a + b) = ca + cb$$

para todos los $a, b, c \in K$.

Entonces, $(K, +, \cdot)$ se llama *anillo*.

La estructura $(K, +)$ se llama *grupo aditivo del anillo*, y $(K, \cdot)$, su *semigrupo multiplicativo*.

Si $(K, \cdot)$ es un monoide, entonces, se dice que $(K, +, \cdot)$ es un *anillo con unidad*.

Al elemento unitario de un anillo, se adopta designarlo con la unidad corriente 1. La existencia del 1 frecuentemente se inserta en la definición de anillo, pero nosotros no haremos eso.

En las aplicaciones y en la teoría general de los anillos (y esa teoría, además, muy desarrollada, existe) se consideran sistemas algebraicos en los cuales, el axioma (K2), o se omite del todo, o bien se reemplaza por otro, en dependencia del problema concreto. En tales casos se habla de *anillos no asociativos*. Por ahora, tendremos sólo anillos comunes (*asociativos*). Esto significa, que podemos basarnos en el teorema 1 del § 1 y no preocuparnos de la colocación de paréntesis en el producto $a_1a_2 \ldots a_k$ de cualquier número k de elementos de un anillo.

El subconjunto L del anillo K se llama *subanillo*, si

$$x,\ y \in L \Rightarrow x - y \in L \text{ y } xy \in L,$$

o sea, si L es subgrupo de un grupo aditivo y subsemigrupo del semigrupo multiplicativo del anillo.

Es claro, que la intersección de cualquier familia de subanillos en K, es un subanillo (el mismo razonamiento que en el caso de los grupos) y, por lo visto, tiene sentido hablar de un subanillo $\langle T \rangle \subset K$, *engendrado por el subconjunto* $T \subset K$. Por definición, $\langle T \rangle$ es la intersección de todos aquellos subanillos en K, que contienen a T. Si desde el principio T fue subanillo, entonces, $\langle T \rangle = T$.

Un anillo se llama *conmutativo*, si $xy = yx$, para todos los $x,\ y \in$ $\in K$ (la diferencia de los grupos, a los anillos conmutativos no se adopta llamarlos abelianos!).

El concepto de anillo, en la forma como fue introducido por nosotros, resulta muy amplio. Más aun, la clase de anillos conmutativos, que a primera vista parece bastante especial, fue objeto de un acentuado estudio en el transcurso de muchas décadas, y en nuestro tiempo la teoría de los anillos conmutativos se entrelaza con la geometría algebraica, una hermosa disciplina matemática que tiene fronteras con el álgebra, la geometría y la topología.

EJEMPLOS. 1) $(\mathbb{Z}, +, \cdot)$ es *el anillo de los números enteros*, con las operaciones ordinarias de suma y de multiplicación. El conjunto $m\mathbb{Z}$ de los números enteros, divisibles por m, será subanillo en $\mathbb{Z}$ (sin unidad, cuando $m > 1$). Análogamente, $\mathbb{Q}$ y $\mathbb{R}$ son anillos con unidad, además, las inclusiones naturales $\mathbb{Z} \subset \mathbb{Q} \subset$ $\subset \mathbb{R}$ definen una cadena de subanillos del anillo $\mathbb{R}$.

2) Las propiedades de las operaciones de suma y de multiplicación en $M_n(\mathbb{R})$ introducidas y exaustivamente estudiadas en el cap. 2, permiten afirmar, que $M_n(\mathbb{R})$ es un anillo con unidad $1 = E$. Se llama *anillo matricial completo sobre* $\mathbb{R}$, y también *anillo de las matrices cuadradas de orden n (o d. dimensiones $n \times n$) sobre* $\mathbb{R}$. Este es uno de los ejemplos más importantes de anillos. Así como para $n > 1$ las matrices, como regla, no son permutables, entonces, $M_n(\mathbb{R})$ es un anillo no conmutativo. El contiene en calidad de subanillos, a los anillos, $M_n(\mathbb{Q})$ y $M_n(\mathbb{Z})$ de las matrices cuadradas del mismo orden, sobre $\mathbb{Q}$ y sobre $\mathbb{Z}$, respectivamente. En general, $M_n(\mathbb{R})$ está saturado de subanillos de todo género. De tiempo en tiempo, algunos de ellos van a aparecer de un modo natural. Notemos también, que se puede considerar el anillo de las matrices cuadradas $M_n(K)$ sobre el anillo conmutativo arbitrario K, por cuanto en caso de suma y de multiplicación de dos matrices $A,\ B \in M_n(K)$, de nuevo se obtendrá una matriz con los coeficientes de K, y las leyes distributivas en $M_n(K)$ resultan

consecuencias de las leyes análogas en K. Todo esto se deduce directamente de las reglas formales de operaciones con matrices, resumidas al final de los puntos 1 y 3 del § 3 del cap. 2.

3) Juntamente con el anillo de las matrices, en distintas partes de las matemáticas es ampliamente usado también el *anillo de las funciones*. Efectivamente, sean, X un conjunto arbitrario, K un anillo arbitrario. Sea, luego, $K^X = \{X \to K\}$ el conjunto de todas las funciones (o, lo que es lo mismo, de las aplicaciones) $f: X \to K$, examinado junto con dos operaciones binarias, *la suma corriente* $f + g$ *y el producto corriente* fg, definidas del siguiente modo:

$$(f + g)(x) = f(x) \oplus g(x),$$
$$(fg)(x) = f(x) \odot g(x)$$

($\oplus$ y $\odot$ son las operaciones de suma y de multiplicación en K). Esto, evidentemente, no es aquella composición (superposición) de funciones, que nos llevó, en el caso de las aplicaciones lineales, al anillo M_n. Más bien, nosotros aquí aceptamos el punto de vista, adoptado en el análisis matemático, cuando, por ejemplo, con $X = \mathbb{R}$, $K = \mathbb{R}$, el producto de las funciones tg y sen será tg $\times$ $\times$ sen: $x \mapsto \text{tg}\, x \cdot \text{sen}\, x$, y no tg $\circ$ sen: $x \mapsto \text{tg}\,(\text{sen}\, x)$.

Sin trabajo se comprueba, que K^X satisface a todos los axiomas de anillo. Así, en vista de la propiedad distributiva de las operaciones en K, tenemos

$$[f(x) \oplus g(x)] \odot h(x) = f(x) \odot h(x) \oplus g(x) \odot h(x)$$

para tres funciones cualesquiera $f, g, h \in K^X$, y cualquier $x \in X$, y esto, por definición de operaciones corrientes, da $(f + g)h = fh + gh$. La veracidad de la segunda ley distributiva se establece análogamente. Si 0, 1, son los elementos cero y unidad en K, entonces

$$0_X : x \mapsto 0, \quad 1_X : x \mapsto 1$$

son las funciones *constantes*, que juegan el rol de cero y de unidad en K^X. En el caso de la conmutatividad de K, el anillo de las funciones K^X también es conmutativo.

El anillo K^X contiene diversos subanillos, definidos por las propiedades especiales de las funciones. Sean, por ejemplo, $X = [0, 1]$ un intervalo cerrado en $\mathbb{R}$ y $K = \mathbb{R}$. Entonces, el anillo $\mathbb{R}^{[0, 1]}$ de todas las funciones reales definidas en $[0, 1]$, contiene en calidad de subanillo al anillo $\mathbb{R}_{ac}^{[0, 1]}$ de todas las funciones acotadas, al anillo $\mathbb{R}_{cont}^{[0, 1]}$ de todas las funciones continuas, al anillo $\mathbb{R}_{dif}^{0, 1}$ de todas las funciones diferenciables continuas, etc., por cuanto, todas las propiedades indicadas se conservan con la suma (resta) y multiplicación de las funciones.

A cada número $a \in \mathbb{R}$ le responde una función *constante* $a_X: x \mapsto a$, y la aplicación de inclusión $a \mapsto a_X$ permite considerar a $\mathbb{R}$ como un subanillo en $\mathbb{R}^X$. En resumen, casi a cada una de las clases naturales de funciones, le corresponde su subanillo en $\mathbb{R}^X$.

4) En cualquier grupo abeliano aditivo $(A, +)$, con la relación $xy = 0$ para todos los $x, y \in A$; se establece la estructura de un anillo con multiplicación nula.

Muchas propiedades de los anillos son reformulaciones de las propiedades correspondientes de los grupos, y, en general, de los conjuntos con una operación asociativa. Por ejemplo, $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ para todos los enteros no negativos m, n y todos los

$a \in K$ (comparar con la relación (2) del § 1). Otras propiedades, más específicas de los anillos, y que se deducen directamente de los axiomas del anillo, conforman, en esencia, las propiedades de $\mathbb{Z}$. Apuntemos algunas de ellas. En primer lugar,

$$a \cdot 0 = 0 \cdot a = 0 \quad \text{para todas las} \quad a \in K. \tag{1}$$

Efectivamente, $a + 0 = a \Rightarrow a(a + 0) = aa \Rightarrow a^2 + a \cdot 0 = a^2 \Rightarrow a^2 + a \cdot 0 = a^2 + 0 \Rightarrow a \cdot 0 = 0$ (análogamente, $0 \cdot a = 0$).

Ahora, supongamos por un momento, que $0 = 1$, obtenemos $a = a \cdot 1 = a \cdot 0 = 0$ para todas las $a \in K$, o sea, K está compuesto solamente de ceros. Por consiguiente, en el anillo no trivial K, siempre $0 \neq 1$. Luego

$$(-a) \cdot b = a(-b) = -(ab), \tag{2}$$

por cuanto, por ejemplo, de (1) y del axioma de propiedad distributiva, sigue

$$0 = a \cdot 0 = a(b - b) = ab + a(-b) \Rightarrow a(-b) = -(ab) \tag{3}$$

Como $-(-a) = a$, entonces, de (2) obtenemos la igualdad $(-a)(-b) = ab$ (por ejemplo, $(-1)(-1) = 1$), $-a = (-1) \cdot a$.

El axioma de distributividad brinda, como su consecuente, la *ley general de la distributividad*

$$(a_1 + \ldots + a_n)(b_1 + \ldots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j, \tag{4}$$

de lo que no es difícil convencerse razonando por inducción, al principio sobre n (para $m = 1$), y luego sobre m. Utilizando ahora (1), (2) y (3), obtenemos

$$n(ab) = (na)b = a(nb)$$

para todas las $n \in \mathbb{Z}$ *y* a, $b \in K$.

Finalmente, indiquemos la fórmula binomial (binomio de Newton)

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}, \tag{5}$$

cierta para todas las a, b, $\in K$, pero sólo en el anillo conmutativo K. Cuando se demuestra (5) es necesario, basándose en (4), operar del mismo modo que en el § 7 del cap. 1, donde se examina el caso particular $K = \mathbb{Z}$.

2. Congruencia. Anillo de las clases de restos. De acuerdo con el teorema 6 del § 2, los subgrupos no nulos del grupo $(\mathbb{Z}, +)$ se completan con los grupos $m\mathbb{Z}$, donde m recorre el conjunto $\mathbb{N}$ de los números naturales. Pero el conjunto $m\mathbb{Z}$, evidentemente, es cerrado no sólo en relación a la operación de suma, sino que también en relación a la operación de multiplicación, cumpliendo con

los tres axiomas del anillo. De este modo, es correcta la siguiente afirmación. Cada subanillo no nulo del anillo $\mathbb{Z}$, tiene la forma $m\mathbb{Z}$ donde $m \in \mathbb{N}$.

Probemos ahora, utilizando el subanillo $m\mathbb{Z} \subset \mathbb{Z}$, de construir un anillo no nulo, compuesto de un número finito de elementos. Con este fin introducimos la

DEFINICION. Dos números enteros n, n' se llaman *congruentes* respecto al mód m (con palabras: *al módulo m*), si al ser divididos por m, dan el mismo resto. Esto se escribe $n \equiv n'$ (m) o $n \equiv n'$ (mód m), y el número m se llama *módulo de congruencia*.

Se obtiene una partición de $\mathbb{Z}$ en clases de números, congruentes entre sí respecto al mód m, denominadas *clases de restos* o residiales respecto al mód m. Cada clase de restos tiene la forma

$$\{r\}_m = r + m\mathbb{Z} = \{r + mk \mid k \in \mathbb{Z}\},$$

así que

$$\mathbb{Z} = \{0\}_m \cup \{1\}_m \cup \ldots \cup \{m-1\}_m. \qquad (6)$$

Observamos, que las clases de restos, son clases adjuntas del grupo aditivo $\mathbb{Z}$ en el subgrupo $m\mathbb{Z}$, y la partición (6) corresponde a la descomposición del teorema 4 del § 2. Por definición, $n \equiv n'$ $(m) \Longleftrightarrow n - n'$ es divisible por m. La comodidad de la escritura $n \equiv n'$ (m) para la relación de divisibilidad $m \mid (n - n')$ consiste en que, con estas congruencias se puede operar exactamente igual que con las igualdades comunes. Y, precisamente, si $k \equiv k'$ (m) y $l \equiv l'$ (m), entonces, $k \pm l \equiv k' \pm l'$ (m) y $kk' \equiv ll'$ (m).

En particular, $k \equiv k'$ $(m) \Rightarrow ks \equiv k's$ (m), para cualquier $s \in \mathbb{Z}$.

De este modo, con cada dos clases $\{k\}_m$ y $\{l\}_m$, independientemente de la elección en ellos de sus representantes k, l, se pueden comparar las clases que resultan ser sus sumas, diferencias, o productos, o sea, en el conjunto $Z_m = \mathbb{Z}/m\mathbb{Z}$ de clases de restos respecto al módulo m, en forma unívoca se inducen las operaciones $\oplus$ y $\odot$:

$$\begin{aligned} \{k\}_m \oplus \{l\}_m &= \{k + l\}_m, \\ \{k\}_m \odot \{l\}_m &= \{kl\}_m. \end{aligned} \qquad (7)$$

Como la definición de estas operaciones se reduce a las operaciones correspondientes sobre los números de las clases de restos, o sea, sobre los elementos de $\mathbb{Z}$, entonces, $\{m\mathbb{Z}, \oplus, \odot\}$ también será un anillo conmutativo con unidad $\{1\}_m = 1 + m\mathbb{Z}$. El se llama anillo de las clases residuales respecto al módulo m. Cuando uno está habituado (y el módulo es dado), el índice m se omite y se escribe $\bar{k}$ en lugar de $\{k\}_m$, así que

$$\bar{k} \oplus \bar{l} = \overline{k + l},$$
$$\bar{k} \odot \bar{l} = \overline{kl}.$$

La etapa superior de adaptación de Z_m, que a primera vista parece sacrílega, pero que representa evidentes ventajas técnicas, se reduce a que se renuncia a los trazos y círculos, y se opera con algún conjunto dado de representantes respecto al módulo m, más frecuentemente con el conjunto $\{0, 1, 2, \ldots, m-1\}$ (se llama *sistema reducido de restos* respecto al módulo m). Digamos, en correspondencia con esta convención, $-k = m - k$, $2(m-1) = -2 = m-2$.

Y bien, los anillos finitos existen. Traemos tres sencillísimos ejemplos, mostrando por separado las tablas de suma y de multiplicación:

Z_2:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Z_3:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Z_4:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	0	2	3
2	0	2	0	2
3	0	3	2	1

El anillo de los restos Z_m desde hace mucho tiempo llamó la atención de los teóricos numeralistas, y en el álgebra sirvió de punto de partida para distintos tipos de generalizaciones.

3. Homomorfismos e ideales de anillos. La aplicación $f: n \mapsto \{n\}_m$ posee, en virtud de (7), las siguientes propiedades: $f(k+l) = f(k) \oplus f(l)$, $f(kl) = f(k) \odot f(l)$. Esto nos da fundamento para hablar del homomorfismo de los anillos $\mathbb{Z}$ y Z_m, de acuerdo con la definición general.

DEFINICIÓN. Sean los anillos $(K, +, \cdot)$ y $(K', \oplus, \odot)$. La aplicación $f: K \to K'$ se llama *homomorfa*, si conserva todas las operaciones, o sea, si

$$f(a+b) = f(a) \oplus f(b),$$
$$f(ab) = f(a) \odot f(b).$$

Además, por supuesto, $f(0) = 0'$ y $f(na) = nf(a)$, $n \in \mathbb{Z}$.

Se llama *núcleo* del homomorfismo f, al conjunto

$$\operatorname{Ker} f = \{a \in K \mid f(a) = 0'\}.$$

Es claro, que $\operatorname{Ker} f$ es un subanillo en K. Pero de ningún modo es éste un subanillo arbitrario. Efectivamente, si $L = \operatorname{Ker} f \subset K$, entonces, $L \cdot x \subseteq L$ (por cuanto $f(lx) = f(l) \odot f(x) = 0' \odot f(x) = 0'$, para todos los $l \in L$) y $x \cdot L \subseteq L$ para todas las $x \in K$. Por

consiguiente, $LK \subset L$ y $KL \subset L$. El subanillo L, que tiene estas propiedades, se llama *ideal* (bilateral) del anillo K. Así, los núcleos de los homomorfismos siempre son ideales.

Al igual que en el caso de los grupos (véase el vocabulario en el punto 3 del § 3), el homomorfismo $f\colon K \mapsto K'$, se llama *monomorfismo*, si $\operatorname{Ker} f = 0$; *epimorfismo*, si la imagen coincide con K':

$$\operatorname{Im} f = f(K) = \{a' \in K' \mid a' = f(a)\} = K',$$

e *isomorfismo*, si la aplicación f es monomorfa y epimorfa. El hecho de isomorfismo de anillos, brevemente se escribe en forma $K \cong K'$.

La aplicación considerada arriba $f\colon n \mapsto \{n\}_m$ resulta, evidentemente, un epimorfismo $\mathbb{Z} \twoheadrightarrow Z_m$ con núcleo $\operatorname{Ker} f = m\mathbb{Z}$. Para la construcción de Z_m en forma implícita, precisamente se utiliza el hecho, de que $m\mathbb{Z}$ es el ideal del anillo $\mathbb{Z}$. Vemos, que en el anillo $\mathbb{Z}$ cada subanillo no nulo es ideal, lo que es una circunstancia casual que no tiene lugar, digamos, ya en el anillo matricial $M_2(\mathbb{Z})$: el conjunto

$$\left\{\begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix} \alpha,\ \beta,\ \delta \in \mathbb{Z}\right\}$$

es un subanillo, pero no ideal, en $M_2(\mathbb{Z})$.

El ejemplo de $m\mathbb{Z}$ sugiere el modo de construcción de ideales (posiblemente, no todos) en el anillo *conmutativo* arbitrario K: si a es algún elemento de K, entonces, el conjunto aK siempre es ideal en K. Efectivamente,

$$ax + ay = a(x + y), \quad (ax)\,y = a(xy).$$

Se dice, que aK es el *ideal principal*, engendrado por el elemento $a \in K$.

Si se toman anillos sólo con unidad, entonces, ideales serán los subgrupos del grupo aditivo del anillo, que sufre multiplicación a la derecha y a la izquierda por los elementos del anillo, y en la definición de homomorfismo $f\colon K \twoheadrightarrow K'$, *es conveniente introducir la condición* $f(1) = 1'$. Cuando existe epimorfismo esta condición, por supuesto, se cumple automáticamente.

Los anillos isomorfos son idénticos por sus propiedades algebraicas, y solamente esas propiedades de los anillos representan un auténtico interés matemático, que se conservan con aplicaciones isomorfas. Precisamente este hecho se tuvo en cuenta, cuando el anillo Z_m se pensó bien como conjunto de las clases de restos respecto al módulo m, bien como conjunto de los representantes de estas clases, elegidos de un modo arbitrario.

4. Conceptos de grupo cociente y de anillo cociente * . Los subgrupos normales de los grupos y los ideales de anillos tienen un

*) En la literatura especializada en idioma español, se usa también el concepto de grupo factor (respectivamente, anillo factor). (Nota del T.)

origen común, ellos son núcleos de homomorfismos. Esta circunstancia halla su expresión en la comunidad de la construcción de formaciones cocientes, en lo que nos proponemos brevemente detenernos. Los detalles ulteriores serán discutidos en la segunda parte del libro.

Comencemos con los grupos. La relación de equivalencia $\sim$ en el grupo G, definida por la descomposición de G en clases adjuntas respecto al subgrupo normal H, tiene una propiedad admirable. Precisamente, si a, b, son elementos arbitrarios del grupo G, y $a \sim c$, $b \sim d$, entonces, por definición (véase la demostración del teorema 4 del § 3), tenemos $a^{-1}c = h_1 \in H$, $b^{-1}d = h_2 \in H$, de donde

$$(ab)^{-1}cd = b^{-1}a^{-1}cd = b^{-1}(a^{-1}c)\,d = b^{-1}h_1b\,(b^{-1}d) = h_1'h_2 \in H$$

y, por consiguiente, $ab \sim cd$. Aquí se usó la propiedad de normalidad de H en G: $b^{-1}h_1b = h_1' \in H$. Así,

$$a \sim c,\ b \sim d \Rightarrow ab \sim cd.$$

De hecho, esto significa, que la operación de multiplicación en el grupo G induce la operación de multiplicación por el conjunto cociente $G/\sim$ (véase el punto 3 del § 6 del cap. 1), al cual convenimos en designarlo con el símbolo G/H.

Tiene sentido hablar sobre la composición (sobre la multiplicación) de los subconjuntos arbitrarios A, B, del grupo G, entendiendo por AB al conjunto de todos los productos ab con $a \in A$, $b \in B$. La asociatividad en G trae consigo la relación

$$(AB)\,C = \{(ab)\,c\} = \{a\,(bc)\} = A\,(BC),$$

y el subconjunto $H \subset G$ es subgrupo en G, exactamente entonces, cuando $H^2 = H$, $H^{-1} = \{h^{-1} \mid h \in H\} \subset H$.

Desde este punto de vista, la clase adjunta aH es igual al producto del conjunto unielemental $\{a\}$ por el subgrupo H. El producto de las clases adjuntas aH, bH, es el conjunto $aH\cdot bH$, el cual, hablando en general, no necesariamente tiene que volver a ser clase adjunta respecto a H. La descomposición S_3 en $H = \{e, (12)\}$, examinada en el punto 4 del § 3, muestra, por ejemplo, que

$$H\cdot(13)\,H = (13)\,H \cup (23)\,H.$$

Una situación totalmente diferente se tiene, cuando H es un subgrupo normal del grupo G. Como $gH = Hg$ para todos los $g \in G$, entonces,

$$aH\cdot bH = a\,(Hb)\,H = a\,(bH)\,H = abH^2 = abH,$$

al mismo tiempo, el razonamiento efectuado arriba muestra, que la clase adjunta abH no depende de los representantes a, b de las clases adjuntas aH, bH. Las propiedades

$$aH\cdot bH = abH,$$
$$H\cdot aH = aH\cdot H = aH,$$
$$a^{-1}H\cdot aH = aH\cdot a^{-1}H = eH = H$$

muestran, que es legítimo el

TEOREMA 1. *Si H es un subgrupo normal en G, entonces, la operación de multiplicación $aH \cdot bH = abH$, dota al conjunto cociente G/H la estructura de un grupo, llamado grupo cociente de G respecto a H. La clase adjunta H sirve de elemento unidad en G/H, y $a^{-1}H = (aH)^{-1}$, es el elemento inverso de aH.* ■

En el caso de un grupo G finito, el orden del grupo cociente G/H se determina por la fórmula

$$|G/H| = \frac{|G|}{|H|} = (G:H),$$

que no causa asombro, luego de todo lo dicho y del teorema de Lagrange (punto 4 del § 3).

En el caso de grupos abelianos escritos aditivamente, la operación binaria en G/H se introduce por medio de la relación

$$(a + H) + (b + H) = (a + b) + H.$$

Correspondientemente, a G/H frecuentemente lo llaman grupo G respecto al módulo H, y en su aplicación al par $G = \mathbb{Z}$, $H = m\mathbb{Z}$ se utiliza también la expresión «grupo $\mathbb{Z}$ respecto al módulo m».

Pasando a la construcción del *anillo cociente* K/L del anillo K por el ideal L, partiremos de que, la «base» del anillo está constituida por un grupo abeliano aditivo. Por esto, como elementos de K/L corresponde tomar las clases adjuntas $a + L$ (llamadas *clases de restos respecto al módulo del ideal* L), la suma de las cuales se efectúa por la regla corriente:

$$(a + L) \oplus (b + L) = (a + b) + L, \qquad (8)$$
$$\ominus (a + L) = -a + L.$$

En calidad de producto de estas mismas clases, tomamos

$$(a + L) \odot (b + L) = ab + L. \qquad (9)$$

Es importante estar convencido, de que este producto está determinado correctamente, o sea, no depende de la elección de los representantes de las respectivas clases. Sean, $a' = a + x$, $b' = b + y$, donde $x, y \in L$. Entonces,

$$a'b' = ab + ay + xb' = ab + z,$$

donde $z = ay + xb' \in L$, por cuanto L es un ideal bilateral. Por esto, $a'b'$ se encuentra en una clase adjunta con el elemento ab, y esto significa, que el producto (9) está correctamente determinado. Para abreviar, hacemos $\bar{a} = a + L$, así que

$$\bar{a} \oplus \bar{b} = \overline{a + b}, \quad \bar{a} \odot \bar{b} = \overline{ab}.$$

En particular, $\bar{0} = L$ y $\bar{1} = 1 + L$ (si la unidad 1 se halla en K). Aún hay que convencerse de que para el conjunto $\bar{K} = K/L = \{\bar{a} \mid a \in K\}$, considerado con las operaciones $\oplus$, $\odot$, se cumplen todos los

axiomas del anillo, pero esto es suficientemente evidente, por cuanto, las operaciones sobre las clases de restos en $\overline{K}$ se reducen a operaciones sobre los elementos de K. Digamos, la distributividad se comprueba así:

$$(\bar{a} \oplus \bar{b}) \odot \bar{c} = \overline{(a+b)} \odot \bar{c} = \overline{(a+b)\,c} = \overline{ac+bc} =$$
$$= \overline{ac} \oplus \overline{bc} = \bar{a} \odot \bar{c} \oplus \bar{b} \odot \bar{c}.$$

Todo esto muestra, que la aplicación

$$\pi : a \mapsto \bar{a}$$

es un epimorfismo de los anillos $K \to K'$, con núcleo $\operatorname{Ker}\pi = L$. Del ejemplo particular del anillo cociente $Z_m = \mathbb{Z}/m\mathbb{Z}$, y del epimorfismo $\mathbb{Z} \to Z_m$, llegamos a situaciones análogas en anillos arbitrarios.

Queda por observar, aunque esto supera los límites de nuestro fin inmediato (explicación de la construcción de Z_m desde el punto de vista del álgebra en general), que todas las imágenes homomorfas del anillo K se agotan, en esencia, con anillos cocientes K respecto a sus correspondientes ideales. Efectivamente, si f: $K \to K'$ es un homomorfismo y $f(K)$, una imagen de K en relación con f, entonces, considerando $f(K) \subset K'$ en lugar de K', llegamos al epimorfismo. A fin de no complicar las designaciones, consideramos desde el principio a f como un epiformismo, o sea, hacemos $f(K) = K'$. De acuerdo con el principio general, expuesto en el punto 3, § 6 del cap. 1, f define la relación de equivalencia de O_f sobre K; en el caso dado, O_f viene expresado por la partición de K en las clases adjuntas $a + \operatorname{Ker} f = C_a$. La aplicación f establece la correspondencia biyectiva f' entre los elementos $a' \in K'$ y las clases C_a, y, precisamente, $f'(C_a) = a'$, si $a' = f(a)$. En este caso

$$f'(C_a + C_b) = f'(C_{a+b}) = f(a+b) = f(a) + f(b) =$$
$$= f'(C_a) + f'(C_b),$$
$$f'(C_a \cdot C_b) = f'(C_{ab}) = f(ab) = f(a) \cdot f(b) = f'(C_a) \cdot f'(C_b),$$

así que la aplicación biyectiva f' es un isomorfismo (para simplificar, las operaciones de suma y de multiplicación en K, en el anillo de las clases de restos $K/\operatorname{Ker} f$ y en K', se designan de la misma manera: $+$ y $\cdot$).

En realidad, hemos demostrado el

TEOREMA 2 (teorema principal sobre homomorfismos de anillos). *Cualquier ideal L del anillo K determina* (con ayuda de las fórmulas (8), (9)) *la estructura del anillo en el conjunto cociente K/L, además, K/L es imagen homomorfa del anillo K con núcleo L. Por el contrario, cada imagen homomorfa $K' = f(K)$ del anillo K, es isomorfa al anillo cociente $K/\operatorname{Ker} f$.*

Observación. El segundo miembro de la fórmula (9), hablando en general, no coincide con el producto de las clases de restos $a + L$ y $b + L$, en el sentido teórico de los conjuntos. Por ejemplo, para $K = \mathbb{Z}$, $L = 8\mathbb{Z}$, el número entero $24 \in 16 + 8\mathbb{Z}$ no está contenido en $(4 + 8\mathbb{Z})^2$, por cuanto $(4 + 8s)(4 + 8t) = 16u$.

5. Tipos de anillos. Campo. En los bien conocidos por nosotros anillos numéricos $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ de $ab = 0$ se deduce, que bien $a = 0$ o $b = 0$. Pero el anillo de las matrices cuadradas M_n ya no tiene estas propiedades. Utilizando la matriz E_{ij} (véase la demostración del teorema 3, § 3 del cap. 2), llegamos a las igualdades $E_{ij}E_{kl} = 0$ para $j \neq k$, aunque, por supuesto, $E_{ij} \neq 0$ y $E_{kl} \neq 0$. Observemos, que $E_{ik}E_{kj} = E_{ij} \neq 0$. Se podía haber atribuido este fenómeno, tan poco común para la aritmética elemental, a la anticonmutatividad del anillo M_n, pero no es así. Como vimos en el punto 2, en el anillo conmutativo Z_4 se cumple la igualdad $2 \odot 2 = 0$, en contra de la notoria verdad «dos por dos son cuatro».

He aquí dos ejemplos más.

EJEMPLO 1. Los pares de números (a, b) $(a, b \in \mathbb{Z}, \mathbb{Q}, \mathbb{R})$ con suma y multiplicación definidas por las fórmulas

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2),$$

forman, evidentemente, un anillo conmutativo con unidad $(1, 1)$, en el que de nuevo nos encontramos con el mismo fenómeno: $(1, 0) \cdot (0, 1) = (0, 0) = 0$.

EJEMPLO 2. En el anillo $\mathbb{R}^{\mathbb{R}}$ de las funciones reales (véase el ejemplo 3 en el punto 1), las funciones $f: x \mapsto |x| + x$ y $g: x \mapsto |x| - x$ son tales, que $f(x) = 0$ para $x \leqslant 0$ y $g(x) = 0$ para $x \geqslant 0$, y por eso, el producto corriente de los mismos fg, será una función nula, aunque $f \neq 0$ y $g \neq 0$.

DEFINICION. Si $ab = 0$ para $a \neq 0$ y $b \neq 0$ en el anillo K, entonces, a se llama *divisor a la izquierda de cero*, y b *divisor a la derecha de cero* (en el anillo conmutativo K sólo se habla de divisores de cero). El propio cero en el anillo $K \neq 0$ es un divisor de cero trivial. Si no hay otros divisores de cero (excepto 0), entonces, K se llama *anillo sin divisores de cero*. El anillo conmutativo con unidad $1 \neq 0$ y sin divisor de cero, se denomina *anillo íntegro* (*anillo de integridad o dominio de integridad*).

TEOREMA 3. *El anillo conmutativo no trivial K con unidad, es íntegro si, y sólo si, en él se cumple la regla de simplificación*:

$$ab = ac, \quad a \neq 0 \Rightarrow b = c$$

para todas las a, b, $c \in K$.

En efecto, si en K tiene lugar la regla de simplificación, entonces, de $ab = 0 = a \cdot 0$ sigue, que bien $a = 0$, o bien $a \neq 0$ pero $b = 0$. Por el contrario, si K es un dominio de integridad, entonces, $ab = ac$, $a \neq 0 \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$. ∎

En el anillo K con unidad, es natural considerar el conjunto de los elementos invertibles: el elemento a se llama *recíproco* (o *divisor de la unidad*), si existe el elemento a^{-1}, para el cual $aa^{-1} = 1 = a^{-1}a$. Más exactamente, se tendría que hablar de elementos *invertibles a la derecha* o *a la izquierda* ($ab = 1$ o $ba = 1$), pero en los anillos conmutativos y también en los anillos sin divisores de ceros, estos conceptos coinciden. Efectivamente, de $ab = 1$, se deduce $aba = a$, de donde $a\,(ba - 1) = 0$. Como $a \neq 0$, entonces, $ba - 1 = 0$, o sea, $ba = 1$.

Sabemos, por ejemplo, que *en el anillo M_n los elementos invertibles son, exactamente, las matrices con determinante distinto de cero*. El elemento recíproco a no puede ser divisor de cero: $ab = 0 \Rightarrow a^{-1}(ab) = 0 \Rightarrow (a^{-1}a)\,b = 0 \Rightarrow 1\cdot b = 0 \Rightarrow b = 0$ (análogamente, $ba = 0 \Rightarrow b = 0$). Por eso no asombra que tenga lugar el

TEOREMA 4. *Todos los elementos invertibles del anillo K con unidad, componen el grupo $U(K)$ respecto a la multiplicación.*

De hecho, como el conjunto $U(K)$ contiene la unidad, y la asociatividad de la multiplicación en K se cumple, entonces, a nosotros nos resta sólo convencernos de que el conjunto $U(K)$ es cerrado, o sea, comprobar que el producto ab de cualesquiera dos elementos a y b de $U(K)$ de nuevo pertenecerá a $U(K)$. Pero, esto es evidente, por cuanto $(ab)^{-1} = b^{-1}a^{-1}$ $(ab\cdot b^{-1}a^{-1} = a\,(bb^{-1})\,a^{-1} = a\cdot 1\cdot a^{-1} = aa^{-1} = 1)$, y, en consecuencia, ab es invertible. ∎

No es difícil ver, que $U(\mathbb{Z}) = \{\pm 1\}$ es un grupo cíclico de orden 2.

Hemos obtenido una clase de anillos muy interesante, los llamados *anillos con divisor*, o *cuerpos*, reemplazando en la definición de anillo al axioma (K2) por la condición, notablemente más fuerte, ($K2'$): en relación a la operación de multiplicación el conjunto $K^* = K \setminus \{0\}$ es un grupo. El anillo con división, por lo visto, no contiene divisores de cero y, en él, cada elemento no nulo es invertible. Las operaciones de suma y de multiplicación se vuelven casi totalmente simétricas en el anillo conmutativo con división, al que se llama *campo*. Pues bien, damos otra vez una

DEFINICIÓN. *El campo P, es un anillo conmutativo que posee unidad $1 \neq 0$, en el cual cada elemento $a \neq 0$ es invertible. El grupo $P^* = U(P)$ se llama grupo multiplicativo del campo.*

El campo se presenta como un híbrido de dos grupos abelianos, uno aditivo y el otro multiplicativo, unidos por la ley distributiva (ahora ya una sola, en vista de la conmutatividad). El producto ab^{-1} se escribe comúnmente en forma *de fracción* (o *de relación, de cociente*) $\frac{a}{b}$, la cual, a fin de economizar espacio en el papel, se designa con la barra transversal a/b. Por consiguiente la fracción a/b, que tiene sentido sólo cuando $b \neq 0$, es la única solución de la ecuación $bx = a$. Las operaciones con fracciones se someten a algunas

reglas

$$
\begin{aligned}
&\frac{a}{b}=\frac{c}{d}\Leftrightarrow ad=bc, && b,\ d\neq 0,\\
&\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, && b,\ d\neq 0,\\
-&\frac{a}{b}=\frac{-a}{b}=\frac{a}{-b} && b\neq 0, \qquad (10)\\
&\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}, && b,\ d\neq 0,\\
&\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}, && a,\ b\neq 0.
\end{aligned}
$$

Estas son reglas «escolares» ordinarias, pero no hay que recordarlas, sino que deducirlas de los axiomas de campo, lo que, por otra parte, no presenta ninguna dificultad. He aquí el razonamiento suficiente para obtener la segunda de las reglas (10). Sean, $x = a/b$ e $y = c/d$, soluciones de las ecuaciones $bx = a$ y $dy = c$. De estas ecuaciones se deduce: $dbx = da$, $bdy = bc \Rightarrow bd\,(x + y) = da + bc \Rightarrow t = x + y = (da + bc)/bd$, única solución de la ecuación $bdt = da + bc$.

Se llama *subcampo* F del campo P, al subanillo en P que es también un campo. Por ejemplo, el campo de los números racionales $\mathbb{Q}$, es un subcampo del campo de los números reales $\mathbb{R}$

En el caso en que $F \subset P$ también se dice, que el campo P es *ampliación* de su subcampo F. De la definición de subcampo se deduce, que el cero y la unidad del campo P también estarán contenidos en F y que van a servir para F de cero y de unidad. Si se toma en P la intersección F_1 de todos los subcampos, contenedores de F y de cierto elemento $a \in P$, no perteneciente a F, entonces, F_1 será el campo mínimo contenedor del conjunto $\{F, a\}$ (el mismo razonamiento que para los grupos en el punto 2 del § 2). Se dice, que la ampliación F_1 del campo F se obtuvo por *adjunción* del elemento a al campo F, y este hecho se refleja en la escritura $F_1 = F\,(a)$. Análogamente, se puede hablar del subcampo $F_1 = F\,(a_1, \ldots, a_n)$ del campo P, obtenido al adjuntar a F n elementos $a_1, \ldots, a_n$ del campo P.

Una pequeña prueba muestra, que $\mathbb{Q}\,(\sqrt{2})$ coincide con el conjunto de los números $a+b\sqrt{2}$, $a, b \in \mathbb{Q}$, por cuanto $(\sqrt{2})^2=2$ y $1/(a+b\sqrt{2})=(a/(a^2-2b^2))-(b/(a^2-2b^2))\sqrt{2}$ para $a+b\sqrt{2}\neq 0$. Lo mismo se refiere a $\mathbb{Q}\,(\sqrt{3})$ $\mathbb{Q}\,(\sqrt{5})$, etc.

Los campos P y P' se llaman *isomorfos*, si son isomorfos como anillos. Por definición, $f\,(0) = 0$ y $f\,(1) = 1'$, para cualquier aplicación isomorfa f. No tiene sentido hablar de homomorfismo de los

campos, porque $\operatorname{Ker} f \neq 0 \Rightarrow f(a) = 0,\ a \neq 0 \Rightarrow f(1) = f(aa^{-1}) = f(a) f(a^{-1}) = 0 \cdot f(a^{-1}) = 0 \Rightarrow f(b) = f(1 \cdot b) = f(1) f(b) = 0 \cdot f(b) = 0,\ \forall b \Rightarrow \operatorname{Ker} f = P$. Por el contrario, los *automorfismos*, o sea, las aplicaciones isomorfas del campo P sobre sí mismo, están vinculadas con las propiedades más profundas de los campos y son un poderoso instrumento para el estudio de estas propiedades, en el marco de la llamada *teoría de Galois.*

El concepto de ampliación de los campos, concuerda plenamente con la eterna tendencia de la humanidad, de incrementar la reserva de números utilizados. El proceso suficientemente lento, el que condicionalmente se representa por medio del diagrama: $\{\text{uno}\} \rightsquigarrow \{\text{uno más uno es dos}\} \rightsquigarrow \mathbb{N} \rightsquigarrow \{\mathbb{N}, 0\} \rightsquigarrow \mathbb{Z} \rightsquigarrow \mathbb{Q} \rightsquigarrow \mathbb{Q}(\sqrt{2}) \rightsquigarrow \mathbb{R}$ y que continúa hasta nuestros días, llevó a una extraordinaria ramificación de la red de campos, muy lejos de los numéricos de costumbre. No todas las etapas de este proceso fueron puramente algebraicas. Digamos, el paso de los números racionales a los *reales*, se basa en los conceptos de continuidad y totalidad (existencia de límites y sucesiones de Cauchy), y hasta ahora se estudia en los cursos de análisis matemático. Al mismo tiempo, una construcción totalmente análoga de los campos de los números p-aditivos, a los cuales aquí no tocamos, y del moderno análisis p-aditivo, desarrollado sobre la base de estos números, son dignas obras de tres ramas, la teoría de los números, el álgebra y el análisis.

6. Característica de un campo. En el punto 2 fue construido el anillo finito de clases de restos Z_m con los elementos

$$\bar{0},\ \bar{1},\ \bar{2},\ \ldots,\ \overline{m-1}$$

y con las operaciones $\bar{k} + \bar{l} = \overline{k+l}$, $\bar{k} \cdot \bar{l} = \overline{kl}$ de suma y de multiplicación (renunciamos a los signos $\oplus$ y $\odot$), Si $m = st$, $s > 1$, $t > 1$, entonces, $\bar{s} \cdot \bar{t} = \bar{m} = \bar{0}$, o sea, $\bar{s}$ y $\bar{t}$ son divisores de cero en Z_m.

Sea ahora $m = p$, un número primo. Se afirma, que Z_p es un campo (de p elementos). Para $p = 2, 3$, esto se ve directamente de las tablas de multiplicación, escritas en el punto 2. En el caso general es suficiente establecer la existencia, para cada $\bar{s} \in Z_p^*$, del elemento inverso $\bar{s'}$ (los números enteros s y s' no deben, evidentemente, dividirse por p).

Consideremos los elementos

$$\bar{s},\ \overline{2s},\ \ldots,\ \overline{(p-1)s}. \qquad (11)$$

Son todos distintos de cero, porque $s \not\equiv 0 \pmod{p} \Rightarrow ks \not\equiv 0 \pmod{p}$, para $k = 1, 2, \ldots, p-1$. Aquí se usa el hecho de que p es primo. Por esta misma razón, los elementos de (11) son todos distintos: de $\overline{ks} = \overline{ls}$, $k < l$, se deduciría que $\overline{(l-k)s} = \bar{0}$, lo que no es

cierto. Así, la sucesión de los elementos de (11) coincide con la sucesión de los, permutados de algún modo, elementos

$$\bar{1}, \bar{2}, \ldots, \overline{p-1}.$$

En particular, se hallará un s', $1 \leqslant s' \leqslant p-1$, para el cual $\overline{s's} = \bar{1}$. Pero esto y significa, que $\bar{s}' \cdot \bar{s} = \bar{1}$, o sea, $\bar{s}'$ es el elemento inverso de s. Hemos demostrado el

TEOREMA 5. *El anillo de clases de restos Z_m es un campo si, y sólo si, $m = p$ es un número primo.* ∎

COROLARIO (pequeño teorema de Fermat). *Para cualquier número entero m, no divisible por el número primo p, tiene lugar la congruencia*

$$m^{p-1} \equiv 1 \ (\text{mód}\ p).$$

DEMOSTRACION. El grupo multiplicativo Z_p^* tiene un orden $p-1$. Por el teorema de Lagrange (véase § 3), $p-1$ se divide por el orden de cualquier elemento de Z_p^*. De este modo, $\bar{1} = (\bar{m})^{p-1} = \overline{m^{p-1}}$, o sea, $\overline{m^{p-1}-1} = \bar{0}$. ∎

No es difícil demostrar el pequeño teorema de Fermat en forma inmediata, con ayuda de la teoría de las congruencias, multiplicando todos los elementos de la sucesión (11).

Los campos Z_2, Z_3, Z_5, ..., tan poco parecidos a los campos, conocidos por nosotros, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{R}$, ocuparon, en la jerarquía algebraica de los campos, un puesto plenamente equiparable, por su significación, con el lugar que desde hace mucho tiempo fue asignado a $\mathbb{Q}$. La cuestión aquí es ésta. Sea P un campo. Como ya hicimos notar, la intersección $\bigcap_i P_i$ de cualquier familia de subcampos $\{P_i \mid i \in I\}$, será subcampo en P.

DEFINICION. *Un campo, que no tiene ningún subcampo propio, se llama primo.*

TEOREMA 6. *En cada campo P se contiene un, y sólo un, campo primo P_0. Este campo primo es isomorfo, bien a $\mathbb{Q}$ o bien a Z_p, para algún p.*

DEMOSTRACION. Suponiendo la existencia de dos subcampos primos distintos P', $P'' \subset P$, necesariamente llegaremos a la conclusión de que la intersección de los mismos $P' \cap P''$ (evidentemente, no vacía, por cuanto 0 y 1 están contenidos tanto en P', como en P''), será un campo, distinto de P' y P''. Esto, sin embargo, no es posible, en virtud de que son primos. Por consiguiente, el subcampo primo $P_0 \subset P$, es único.

En P_0, juntamente con el elemento unidad 1, están contenidos todos sus múltiplos $n \cdot 1 = 1 + \ldots + 1$. De las propiedades generales de las operaciones de suma y de multiplicación de los elementos en los anillos (véase el final del punto 1) se deduce, que

$$s \cdot 1 + t \cdot 1 = (s+t) \cdot 1, \quad (s \cdot 1)(t \cdot 1) = (st) \cdot 1, \quad s, t \in \mathbb{Z} \qquad (12)$$

Por eso, la aplicación f del anillo $\mathbb{Z}$ en P, definida por la regla $f(n) = n1$, es un homomrfismo cuyo núcleo, siendo ideal en $\mathbb{Z}$, tiene la forma $\operatorname{Ker} f = m\mathbb{Z}$. Si $m = 0$, entonces, f es un isomorfismo, y las fracciones $(s \cdot 1)/(t \cdot 1)$, que tienen sentido en P (por cuanto P es un campo), forman el campo P_0, isomorfo a $\mathbb{Q}$, que será un subcampo primo en P.

Y si $m > 0$, entonces, evidentemente, la aplicación f^* definida por la regla

$$f^*: \bar{k} = \{k\}_m \mapsto f(k),$$

será una inclusión isomorfa $Z_m \to P$. Por el teorema 5, esto sólo es posible cuando $m = p$ es un número primo. Por consiguiente, $f^*(Z_p)$ es un subcampo primo en P. ∎

DEFINICION. Se dice, que el campo P tiene *característica cero*, si su subcampo primo P_0 es isomorfo a $\mathbb{Q}$; P es un campo *primo* (*o finito*) *de característica* p, si $P_0 \cong Z_p$. Se escribe char $P = 0$ o char $P = p > 0$, respectivamente.

En lugar de Z_p, para designar al campo «abstracto» de p elementos, se usa habitualmente $\mathbb{F}_p$, o GF (p) (*Galois Field: campo de Galois*). Hay que tener en cuenta, que existe un campo finito GF (q) con $q = p^n$ elementos, donde p es primo y n cualquier número entero positivo. A esta interesante cuestión regresaremos en el cap. 9, pero ahora nos limitamos sólo a un ejemplo de un campo de cuatro elementos $\{0, 1, \alpha, \beta\}$:

GF (4):

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Qué son α y β por el momento no nos interesa. Se recomienda verificar el cumplimiento de la ley distributiva.

A veces, a la característica nula la llaman infinita, en correspondencia con su interpretación como orden del elemento 1 en el grupo aditivo del campo P. Análogamente, la característica finita p es el orden común de cualquier elemento no nulo en el grupo aditivo:

$$px = x + \ldots + x = p(1 \cdot x) = 1 \cdot x + \ldots + 1 \cdot x = \\ = (1 + \ldots + 1)\, x = (p \cdot 1)\, x = 0.$$

7. Observación sobre sistemas lineales. Ha llegado la hora de dar una ojeada mental a la teoría de los sistemas de ecuaciones lineales, expuesta en los capítulos anteriores, y a la, derivada de ella,

teoría de determinantes. Como coeficientes en las ecuaciones lineales y como elementos de matrices, teníamos números, racionales o reales, pero lo específico de estos números no se utilizó de ningún modo. No hay ningún obstáculo para tomar ahora, en lugar de los números, a los elementos del campo dado P. Al mismo tiempo, los resultados también deberán de formularse en términos del campo P: los componentes de la solución del sistema lineal y los valores de la función det pertenecerán a P. El método de Gauss para resolver sistema de ecuaciones lineales, la teoría de determinantes, la regla de Cramer, siguen siendo legítimos (sin cambios fundamentales) para el campo arbitrario P.

EJEMPLO 1. Sea dado un sistema homogéneo de ecuaciones lineales $AX = 0$, con la matriz cuadrada

$$A = (a_{ij}) = \begin{Vmatrix} 1 & 2 & 3 & 4 \\ -10 & 13 & 14 & 15 \\ 12 & -9 & 14 & 15 \\ 12 & 13 & -8 & 15 \end{Vmatrix}$$

y con la columna de incógnitas $X = [x_1, x_2, x_3, x_4]$. Cálculos directos muestran, que $\det A = 2^3 \cdot 11^4$. Por consiguientte, con a_{ij}, $x_k \in P$, donde P es un campo cualquiera de característica cero, o de característica $p \neq 2, 11$ (en este caso los números enteros $1, 2, 3, 4, -10, \ldots, 15$ se reemplazan por las correspondientes clases de restos), el sistema es determinado y tiene solamente una solución trivial $X = 0$.

Si char $P = 2$ (digamos, $P = Z_2$), entonces, de la congruencia

$$\begin{Vmatrix} 1 & 2 & 3 & 4 \\ -10 & 13 & 14 & 15 \\ 12 & -9 & 14 & 15 \\ 12 & 13 & -8 & 15 \end{Vmatrix} \equiv \begin{Vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{Vmatrix} \pmod{2}$$

llegamos a la conclusión, de que el rango del sistema es igual a dos, y el sistema admite dos soluciones independientes $X_1 = [1, 0, 1, 0]$, $X_2 = [0, 1, 0, 1]$. Para evitar confusiones se tendría que haber escrito $X_1 = [\bar{1}, \bar{0}, \bar{1}, \bar{0}]$, $X_2 = [\bar{0}, \bar{1}, \bar{0}, \bar{1}]$, pero nos consideramos lo suficientemente preparados como para comprender la escritura simplificada.

Si char $P = 11$, entonces, de la congruencia

$$\begin{Vmatrix} 1 & 2 & 3 & 4 \\ -10 & 13 & 14 & 15 \\ 12 & -9 & 14 & 15 \\ 12 & 13 & -8 & 15 \end{Vmatrix} \equiv \begin{Vmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{Vmatrix} \pmod{11}$$

se deduce, que el sistema tiene tres soluciones independientes

$$X_1 = [9, 1, 0, 0], \quad X_2 = [8, 0, 1, 0], \quad X_3 = [7, 0, 0, 1].$$

Como vemos, la respuesta depende esencialmente del campo considerado P, pero el análisis del sistema en nada se diferencia del corriente. Por consiguiente, una de las ventajas del paso de $\mathbb{R}$ y $\mathbb{Q}$ a un campo arbitrario, se reduce a la eliminación del doblaje de

los razonamientos análogos. Pero, además, se tienen causas de más peso.

Hablando sobre un grupo lineal completo, hasta el momento lo consideramos como el grupo de todas las matrices no degeneradas, con coeficientes de $\mathbb{Q}$ o de $\mathbb{R}$. El conjunto de las matrices cuadradas de dimensiones $n \times n$ con coeficientes en un campo arbitrario P, compone el anillo de matrices $M_n(P)$, y el subconjunto de todas las matrices no degeneradas $A \in M_n(P)$ (de matrices con $\det A \neq 0$) lleva al concepto de grupo lineal completo $GL(n, P)$ sobre el campo P. Variando el campo P, por ejemplo, haciendo $P = \mathbb{F}_p$, se puede, de un modo natural, obtener una serie de grupos importantes (véase el cap 7).

Los campos del tipo $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ y otros, se llaman habitualmente *campos numéricos*. El campo $\mathbb{F}_p$ es un ejemplo de campo no numérico: no sería correcto llamar a sus elementos números por el sólo hecho de que ellos frecuentemente se identifican con los elementos del conjunto $\{0, 1, \ldots, p-1\}$.

En el § 2 del cap 1 se planteó el problema (con el número 3) de la utilización de los campos finitos en la teoría de la codificación. Formularemos ahora un pequeño ejemplo sobre este tema.

EJEMPLO 2 Para la transmisión de la consigna MIRU MIR*) en principio es suficiente la repetición de cuatro informaciones elementales, $M = (0, 0)$, $I = (1, 0)$, $R = (0, 1)$, $U = (1, 1)$, interpretadas como vectores-filas del espacio lineal bidimensional $\mathbb{F}^2$ sobre el campo $\mathbb{F}_2 \cong Z_2 = \{0, 1\}$ de dos elementos. Pero, durante el tiempo de trasmisión, en el canal de comunicación aparecen perturbaciones (cambios del símbolo 0 por el 1, o del 1 por el cero), como resultado de las cuales, en la recepción al final del canal puede llegar, por ejemplo, la información RIMU RIM. De acuerdo al teorema fundamental de Shennon, a cuenta del aumento de la longitud de las informaciones elementales (o sea, a cuenta de la velocidad de trasmisión), la acción de las perturbaciones es eliminable. Sea, digamos, que de las condiciones de trasmisión es sabido, que en cada información elemental de longitud cinco, no se produce más de una tergiversación. Tomamos entonces en el espacio $S = \mathbb{F}_2^5$, el subconjunto $S_0 = \{M = (0, 0, 1, 1, 0), I = (1, 0, 0, 1, 1), R = (0, 1, 1, 0, 1), U = (1, 1, 0, 0, 0)\}$ de los llamados *vectores de códigos*. De la tabla

Vectores de códigos	00110	10011	01101	11000
Vectores, obtenidos de los vectores de códigos, como resultado de tergiversaciones	00010 00100 00111 01110 10110	00011 10001 10010 10111 11011	00101 01001 01100 01111 11101	01000 10000 11100 11001 11010

se ve, que los conjuntos de vectores tergiversados de distintas columnas, no se intersecan, y, por consiguiente, es posible una decodificación correcta, o sea, el restablecimiento de una comunicación veraz.

*) En ruso: ¡Paz al mundo!

Hemos obtenido *el cod S_0, que corrige un error*. Pasando al espacio $\mathbb{F}_2^n$ de dimensión n suficientemente grande, se puede construir un código análogo, capaz de transmitir sin errores todo el alfabeto, o sea, cualquier texto. A fin de que la decodificación no se transforme en una selección larga y muy lenta, hay que eligir a S_0 de un modo especial. Para esto existe una serie de procedimientos, entre ellos y puramente algebraicos, basados en el uso de los campos finitos $\mathbb{F}_q$.

EJERCICIOS

1. Desarrollando la idea del ejemplo 2) del § 1, mostrar, que el conjunto $\mathcal{P}(\Omega)$ con las operaciones

$$A+B=(A\cup B)\setminus(A\cap B),\quad AB=A\cap B;\quad A,\ B\in\Omega,$$

es un anillo con unidad, y todos los elementos de su grupo aditivo son de orden 2.

2. Establecer la conmutatividad de un anillo arbitrario, en el cual, cada elemento x satisface a la ecuación $x^2=x$. ¿Es cierto esto para la condición $x^3=x$?

3. ¿Son isomorfos los campos $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$?

4. ¿Forman un ideal los elementos no invertibles de los anillos: 1) Z_{16} 2) Z_{21}?

5. Mostrar, que la imagen epimórfica del anillo conmutativo, es un anillo conmutativo.

6. Si K es un anillo con unidad y L un ideal, entonces, el anillo cociente K/L también tiene unidad.

7. Cualquier anillo entero finito K, es un campo.

8. Sean, p un número primo, y K un anillo conmutativo con unidad, tal que, $px=0$ para todos los $x\in K$. Mostrar que, entonces

$$(x+y)^{p^m}=x^{p^m}+y^{p^m},\quad m=1,\ 2,\ \ldots$$

(*Indicación*. Utilizar la inducción sobre m, y la circunstancia de que el coeficiente binomial $\binom{p}{k}$, $0<k<p$, es divisible por p).

9. Demostrar, que el anillo K, compuesto de cinco elementos, o es isomorfo a Z_5, o bien es anillo con multiplicación nula.

10. El conjunto de las matrices triangulares superiores $T=\left\{\left\|\begin{matrix}a & c\\ 0 & b\end{matrix}\right\| \mid a,\ b\in\mathbb{Z}\right\}$, forma un subanillo en $M_2(\mathbb{Z})$. Convencerse de esto y hacer una descripción de los ideales del anillo T.

11. El elemento $x\neq0$ del anillo K se llama *nilpotente*, si $x^n=0$, para algún $n\in\mathbb{N}$. Mostrar, que:

(i) la nilpotencia del elemento x conlleva a la invertibilidad del elemento $1-x$ en cualquier anillo con unidad;

(ii) el anillo $\mathbb{Z}_m=\mathbb{Z}/m\mathbb{Z}$ contiene elementos nilpotentes, exactamente entonces, cuando m es divisible por el cuadrado de un número natural >1.

12. Demostrar, que en el anillo conmutativo K, con unidad y con potencia infinita $|K|$, no puede haber un número finito $n\geqslant1$ de elementos no invertibles $\neq0$. (*Indicación*. Usar el razonamiento por el contrario. Sea $N=\{a_1,\ldots,a_n\}$, el conjunto de todos los elementos no invertibles $\neq0$ del anillo K. La aplicación $\rho_x: a_i\mapsto xa_i$, es una biyección de $N\to N$ para cualquier $x\in K\setminus(N\cup\{0\})$. El núcleo Ker ρ de la aplicación $\rho: x\mapsto\rho_x$ es infinito.)

13. Sean, un anillo asociativo arbitrario K, con unidad 1, y a, b, elementos del mismo. Mostrar, que

$$(1-ab)c=1=c(1-ab)\Rightarrow(1-ba)d=1=d(1-ba),$$

donde, $d = 1 + bca$, o sea, la invertibilidad de $1 - ab$ en K, lleva a la invertibilidad $1 - ba$. ¿A qué es igual el elemento $1 + adb$?

14. Mostrar, que las matrices $\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix}$ con a, $b \in Z_3$, forman un campo de 9 elementos, y que el grupo multiplicativo de este campo, es cíclico, de orden 8.

15. ¿Es capaz o no el código S_8 (del ejemplo 2, al final del parágrafo) de corregir dos errores?

Capítulo 5

NUMEROS COMPLEJOS Y POLINOMIOS

En este capítulo serán considerados sistemas algebraicos totalmente concretos, parcialmente conocidos de las matemáticas escolares, pero que merecen ser objeto de una atención un poco más detallada. El punto de vista elaborado en el capítulo anterior, nos permite dirigir una mirada fresca al tradicional «campo de actividad» del álgebra de los siglos pasados. Al mismo tiempo, en el ejemplo de los polinomios, se harán más comprensibles y tangibles tales problemas, como la ampliación de los anillos y la univocidad de la descomposición en multiplicadores primos, en los anillos íntegros (dominios de integridad).

§ 1. CAMPO DE LOS NÚMEROS COMPLEJOS

Una obstinación, digna de la mejor imitación, en la historia de las matemáticas, se observa en la larga lucha entre los defensores y enemigos de los números «imaginarios», como fuente de los cuales sirve la ecuación algebraica

$$x^2 + 1 = 0. \tag{1}$$

Se puede ocupar una posición simplista, limitándose a la escritura formal de las soluciones de la ecuación (1), en forma de $\pm \sqrt{-1}$. Pero esto no era difícil hacerlo en tiempos más lejanos; sólo quedaba darle sentido a la escritura indicada. Resolveremos este problema a distintos niveles. Al principio, introducimos algunas reflexiones eurísticas.

1. Construcción auxiliar. Deseamos ampliar el campo de los números reales $\mathbb{R}$ de tal modo, que, en el nuevo campo, la ecuación (1) tenga solución. Un modelo de esta ampliación puede ser el conjunto P de todas las matrices cuadradas

$$\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix} \in M_2(\mathbb{R}). \tag{2}$$

Se afirma, que P es un campo (comparar con el ejercicio 14 del § 4, cap. 4).

Efectivamente, en P están contenidos el cero 0 y la unidad E del anillo $M_2(\mathbb{R})$.

Luego, de las relaciones

$$\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix} + \begin{Vmatrix} c & d \\ -d & c \end{Vmatrix} = \begin{Vmatrix} a+c & b+d \\ -(b+d) & a+c \end{Vmatrix},$$

$$-\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix} = \begin{Vmatrix} -a & -b \\ -(-b) & -a \end{Vmatrix}, \qquad (3)$$

$$\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix}\begin{Vmatrix} c & d \\ -d & c \end{Vmatrix} = \begin{Vmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{Vmatrix}$$

se deduce que P es cerrado con respecto a las operaciones de suma y multiplicación. La asociatividad de estas operaciones, es consecuencia de sus asociatividades en M_2. Lo mismo se refiere a las leyes de distributividad. De este modo, P es un subanillo en M_2. Queda por demostrar la existencia en P de una matriz inversa a cualquier matriz (2), con determinante $\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix} = a^2 + b^2 \neq 0$ (la conmutatividad de P se desprende de la fórmula (3)). Directamente, de la fórmula para los coeficientes de la matriz inversa (véase el teorema 1, § 3 del cap. 3), o por medio de la resolución del sistema lineal

$$ax - by = 1,$$
$$bx + ay = 0,$$

que surge de la condición

$$\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix}\begin{Vmatrix} x & y \\ -y & x \end{Vmatrix} = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix},$$

hallamos, que

$$\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix}^{-1} = \begin{Vmatrix} c & d \\ -d & c \end{Vmatrix}, \text{ donde } c = \frac{a}{a^2+b^2}, \quad d = \frac{-b}{a^2+b^2}. \qquad (4)$$

Utilizando la regla (5) del § 3, cap. 2, de multiplicación de matrices por números, cualquier elemento del campo P lo anotamos en la forma

$$\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix} = aE + bJ, \text{ donde } a,\ b \in \mathbb{R},\ J = \begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}. \qquad (5)$$

El campo P contiene el subcampo $\{aE \mid a \in \mathbb{R}\} \cong \mathbb{R}$, y la relación

$$J^2 + E = 0$$

muestra, que el elemento $J \in P$ «con exactitud hasta el isomorfismo» es solución de la ecuación (1). Aquí no se puede hablar de ninguna mística acerca del «elemento imaginario J».

Sin embargo, se llama campo de los números complejos, no el campo P, sino un cierto objeto isomorfo del mismo, cuyos elementos se representan como puntos de un plano. El deseo de tener una realización geométrica del campo P no es casual, si se recuerda, que el campo $\mathbb{R}$ para nosotros es inseparable de la «recta real», con un punto

dado, representante del cero, y una escala determinada, que define la situación del número 1.

2. Plano complejo. Y bien, queremos construir un campo $\mathbb{C}$ cuyos elementos sean puntos del plano $\mathbb{R}^2$, siendo que la suma y multiplicación de los puntos, sometiéndose a todas las reglas de operaciones en un campo, resuelvan nuestro problema. Elegimos en el plano cartesiano, un sistema de coordenadas cartesianas, con eje de abscisas x y con eje de ordenadas y. Escribimos (a, b) para indicar el punto con abscisa a y ordenada b. Para los puntos (a, b) y (c, d), definimos la suma y el producto por las reglas

$$\begin{gathered}(a, b) + (c, d) = (a + c, b + d), \\ (a, b)(c, d) = (ac - bd, ad + bc)\end{gathered} \tag{6}$$

(el uso de los mismos signos $+$, $\cdot$, que en el campo $\mathbb{R}$, no debe de llevar a confusión). Una comprobación directa, pero bastante fatigosa, nos convencería de que las operaciones así definidas dotan al conjunto de pares (de puntos en el plano) para la construcción de un campo con las propiedades necesarias. No hay necesidad, por suerte, de esta comprobación. La comparación

$$(a, b) \mapsto \left\| \begin{matrix} a & b \\ -b & a \end{matrix} \right\|$$

de los puntos del plano $\mathbb{C}$ con los elementos del campo P, anteriormente construido, y una ligera mirada a las fórmulas (3) y (6), nos convencen de que estamos en presencia de un isomorfismo y que, por consecuencia, el conjunto $\mathbb{C}$ es un campo. Este es el que se llama habitualmente campo de los números complejos. Teniendo en cuenta la realización geométrica de este campo, $\mathbb{C}$ también se denomina *plano complejo.*

El eje de abscisas elegido por nosotros, o sea, el conjunto de puntos $(a, 0)$, no se diferencia en nada, por sus propiedades, de la recta real, y suponemos $(a, 0) = a$. El cero $(0, 0)$ y la unidad $(1, 0)$ del campo se hacen, con esto, números reales corrientes. Para el punto $(0, 1)$ en el eje de ordenadas se introduce por tradición la designación i «unidad imaginaria», que es la raíz de la ecuación (1): $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$. El número complejo arbitrario $z = (x, y)$, se escribe ahora en la forma acostumbrada

$$z = x + iy, \quad x, \quad y \in \mathbb{R}, \tag{7}$$

sumamente cercana a la forma (5) de los elementos del campo P. Notemos, que $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Por eso, $\mathbb{C}$ es un campo con característica nula (véase punto 6, § 4, cap. 4).

3. Interpretación geométrica de las operaciones con números complejos. El eje de abscisas del plano complejo, se llama habitualmente eje *real*; el eje de ordenadas, eje *imaginario*, y los números iy, ubicados sobre el mismo, números *puramente imaginarios*, aunque

la palabra «*imaginario*» perdió su sentido inicial. Correspondientemente en la escritura (7), x es la *parte real*, *e* iy la *parte imaginaria* del número complejo z. Examinemos la imagen, que confronta a cada número complejo $z = x + iy$, con su complejo conjugado $\bar{z} = x - iy$ (*operación de conjugación compleja*). Geométricamente, ello se reduce al reflejo del plano complejo con relación al eje real (véase fig. 15). Es sumamente notable, la legitimidad del

TEOREMA 1. *La aplicación $z \mapsto \bar{z}$ es un automorfismo de orden 2 del campo* $\mathbb{C}$, *que deja en su lugar a todos los números reales. La suma*

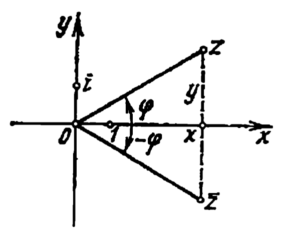


Fig. 15

y el producto de números complejos conjugados dan como resultado números reales.

DEMOSTRACION. La afirmación $\bar{x} = x$, $x \in \mathbb{R}$, es evidente de la definición de número complejo conjugado. En particular, $\bar{0} = 0$ y $\bar{1} = 1$. Es igualmente evidente la afirmación sobre el orden: $\overline{(\bar{z})} = z$. Nos quedan por comprobar las relaciones

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \quad \overline{z_1 z_2} = \bar{z}_1 \cdot \bar{z}_2, \tag{8}$$

pero ellas se deducen directamente de las fórmulas (6), que sólo deben ser escritas de nuevo, en la forma

$$(x_1 + iy_1) + (x_2 + iy_2) = (x_1 + x_2) + i\,(y_1 + y_2), \tag{9}$$
$$(x_1 + iy_2) \cdot (x_2 + iy_2) = (x_1 x_2 - y_1 y_2) + i\,(x_1 y_2 + x_2 y_1).$$

Un caso particular de las fórmulas (9), es la afirmación sobre la suma y el producto del número $z = x + iy$, y su complejo conjugado $\bar{z}$: $z + \bar{z} = 2x$, $z\bar{z} = x^2 + y^2$. ∎

Observación. El automorfismo $z \mapsto \bar{z}$ se distingue de muchos otros automorfismos del campo $\mathbb{C}$ en que, él es el único continuo (que traslada los puntos cercanos al plano $\mathbb{C}$ a sus proximidades). No haremos más precisa ni demostraremos esta afirmación.

Se llama *módulo* (o *valor absoluto*) de un número complejo $z = x + iy$, el número real no negativo $|z| = \sqrt{z\bar{z}} = \sqrt{x^2 + y^2}$

La posición del punto z en el plano, como es sabido, queda totalmente determinada prefijando sus coordenadas polares: la distancia $r = |z|$ desde el origen de las coordenadas hasta z, y el ángulo φ entre el sentido positivo del eje de abscisas y el sentido del origen de las coordenadas a z (fig. 15). El ángulo φ se llama *argumento* del número z, y se designa con el símbolo $\arg z = \varphi = \operatorname{arctg} y/x$. Por

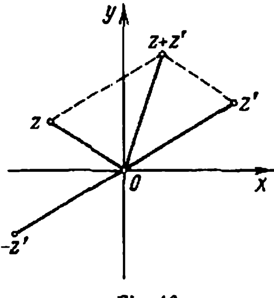


Fig. 16

definición, el arg z puede tener cualquier valor positivo o negativo, pero con r dado, los ángulos que se diferencian en múltiplos enteros de 2π, corresponden a un mismo número. No está definido el argumento para el número 0, con módulo $|0| = 0$. Las relaciones de «mayor» o «menor» carecen de sentido cuando se refieren a números complejos, o sea, a estos no se los puede unir con el signo de desigualdad: a diferencia de los números reales, el argumento de los cuales adopta sólo dos valores principales, 0 (números positivos) y π (números negativos), los *números complejos no están ordenados.*

Las coordenadas polares r y φ determinan a x e y por las conocidas fórmulas

$$x = r \cos \varphi, \quad y = r \operatorname{sen} \varphi, \quad z = r (\cos \varphi + i \operatorname{sen} \varphi). \tag{10}$$

Esta es, la llamada *forma trigonométrica* del número z.

La operación de adición de los números complejos z, z' se expresa sencillamente en coordenadas cartesianas, precisamente, por la regla del paralelogramo, o, lo que es equivalente, por la regla de adición de segmentos orientados (vectores), que parten del origen de las coordenadas y que corresponden a los números z y z' (fig. 16). De este mismo dibujo, comparando los lados del triángulo con vértices en los puntos 0, z y $z + z'$ (e identificando los valores absolutos con las longitudes geométricas correspondientes), obtenemos la importante desigualdad

$$|z + z'| \leqslant |z| + |z'|. \tag{11}$$

Observemos, que la desigualdad (11), que podría haber sido escrita en la forma más general

$$|z| - |z'| \leqslant |z \pm z'| \leqslant |z| + |z'|,$$

es totalmente análoga a la correspondiente desigualdad para los números reales.

La operación de multiplicación de números complejos, es cómodo expresarla en coordenadas polares.

TEOREMA 2. *El módulo del producto de los números complejos* z, z', *es igual al producto de sus módulos, y el argumento, es igual a la*

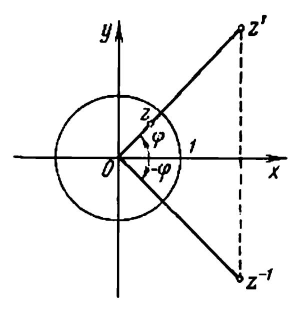


Fig. 17

suma de los argumentos de los factores

$$|zz'| = |z|\cdot|z'|, \quad \arg zz' = \arg z + \arg z'. \qquad (12)$$

Análogamente, $|z/z'| = |z|/|z'|$, $\arg z/z' = \arg z - \arg z'$.

DEMOSTRACION. Efectivamente, sea la forma trigonométrica

$$z = r(\cos\varphi + i \operatorname{sen}\varphi), \quad z' = r'(\cos\varphi' + i \operatorname{sen}\varphi').$$

Por multiplicación directa, o por la fórmula (9), obtenemos

$$zz' = rr'\,[(\cos\varphi\cos\varphi' - \operatorname{sen}\varphi\operatorname{sen}\varphi') +$$
$$+\, i(\cos\varphi\operatorname{sen}\varphi' + \operatorname{sen}\varphi\cos\varphi')],$$

y esta relación, con ayuda de conocidas fórmulas, conduce a la forma trigonométrica del número zz': ∎

$$zz' = |z|\cdot|z'|\cdot[\cos(\varphi + \varphi') + i\operatorname{sen}(\varphi + \varphi')).$$

Si, luego, $z'' = z/z'$, entonces, $z = z'z''$. Por eso, utilizando las ya demostradas fórmulas (12) para el producto $z'z''$, obtenemos de ellas las fórmulas para la fracción z/z'.

En particular, $z^{-1} = |z|^{-1}[\cos(-\varphi) + i\operatorname{sen}(-\varphi)]$. Para obtener z^{-1} en el plano complejo (fig. 17), hay que, por lo tanto, aplicar a z una inversión respecto a la circunferencia con radio unitario

y centro en 0 (esto da el punto z'), y, luego, el reflejo con respecto al eje real (o el automorfismo $z' \mapsto \overline{z'}$).

De hecho, las afirmaciones sobre el módulo del producto y el módulo de la adición se deducen fácilmente, sin recurrir a la intuición geométrica, del teorema 1. En efecto, en primer lugar,

$$|zz'|^2 = zz'\overline{zz'} = zz'\bar{z}\bar{z}' = z\bar{z}\cdot z'\bar{z}' = |z|^2|z'|^2,$$

de donde $|zz'| = |z|\cdot|z'|$. Luego, observando, que $|z| = \sqrt{x^2+y^2} \geqslant \sqrt{x^2} = |x|$, obtenemos

$$|1+z|^2 = (1+z)(1+\bar{z}) = 1+(z+\bar{z})+z\bar{z} =$$
$$= 1+2x+|z|^2 \leqslant 1+2|z|+|z|^2 = (1+|z|)^2.$$

De los resultados obtenidos, podemos sacar cierto principio general: la forma corriente (7) de los números complejos, se ha adaptado para la expresión de sus propiedades aditivas; y la forma trigonométrica (10), para la expresión de sus propiedades multiplicativas. La inobservancia de este principio lleva a fórmulas extremadamente difíciles, que obscurecen la esencia de la cosa.

4. Elevación a potencias y extracción de raíces. De la fórmula (12) para la multiplicación de números complejos, dados en forma trigonométrica, se deduce la llamada *fórmula de Moivre*

$$[r(\cos\varphi + i \operatorname{sen}\varphi)]^n = r^n(\cos n\varphi + i \operatorname{sen} n\varphi), \tag{13}$$

legítima para todos los $n \in \mathbb{Z}$ (en otra escritura: $|z^n| = |z|^n$, $\arg z^n = n\cdot\arg z$). El caso particular de la fórmula (13) para $r = 1$, la fórmula binomial (1) del § 7 del cap. 1, y las relaciones

$$i^2 = -1,\quad i^3 = -i,\quad i^4 = 1,\quad i^{4k+l} = i^l$$

hacen posible obtener la expresión de los senos y cosenos del ángulo múltiplo:

$$\begin{aligned} \cos n\varphi &= \sum_{k\geqslant 0} (-1)^k \binom{n}{2k} \cos^{n-2k}\varphi\cdot\operatorname{sen}^{2k}\varphi,\\ \operatorname{sen} n\varphi &= \sum_{k\geqslant 0} (-1)^k \binom{n}{2k+1} \cos^{n-1-2k}\varphi\cdot\operatorname{sen}^{2k+1}\varphi. \end{aligned} \tag{14}$$

En honor a la verdad, cabe anotar, que el caso particular de la fórmula (14) para $n = 2$ fue utilizado antes por nosotros, en el curso de la demostración del teorema 2.

Observación. Sea $e^{\alpha} = \lim\limits_{n\to\infty}\left(1+\frac{\alpha}{n}\right)^n$. En el análisis se demuestra, por medio del desarrollo de las funciones de la variable compleja en series exponenciales, *la fórmula de Euler*

$$e^{i\varphi} = \cos\varphi + i\operatorname{sen}\varphi. \tag{15}$$

de la cual se desprenden todos los resultados obtenidos por nosotros. Queda sólo por observar, que

$$e^{i\varphi}e^{i\varphi'} = e^{i(\varphi+\varphi')}, \quad (e^{i\varphi})^n = e^{in\varphi}.$$

La forma trigonométrica del número complejo z, se reduce a la escritura

$$z = |z| \cdot e^{i\varphi}.$$

Luego, quisiéramos aprender a extraer raíces de cualquier grado de los números complejos, y la principal pregunta que aquí surge es: ¿siempre es posible hacerlo? Resulta que siempre, y la fórmula de Moivre da, en esencia, la solución total de esta cuestión. Seanos dado el número complejo $z = r(\cos\varphi + i \operatorname{sen}\varphi)$, y queremos hallar un número $z' = r'(\cos\varphi' + i\operatorname{sen}\varphi')$ tal, que $(z')^n = z$. Expresando $(z')^n$ por la fórmula de Moivre, y comparando luego en ambos miembros de la igualdad $(z')^n = z$ los módulos y los argumentos, hallamos que $(r')^n = r$ y que $n\varphi' = \varphi + 2\pi k$ (el sumando $2\pi k$ es el pago por la determinación incompleta del argumento). Así,

$$r' = \sqrt[n]{r}, \quad \varphi' = \frac{\varphi + 2\pi k}{n}$$

(por $\sqrt[n]{r}$ se sobreentiende el valor aritmético de la raíz de n-ésimo grado de un número real positivo). La raíz $\sqrt[n]{z}$, por lo visto, existe, pero está diterminada no unívocamente. Para $k = 0, 1, \ldots, n-1$ se obtendrán n valores distintos de z', además, ellos agotan todas las raíces, por cuanto, de $k = nq + r$, $0 \leqslant r \leqslant n-1$, se desprende que

$$\varphi' = \frac{\varphi + 2\pi k}{n} + 2\pi q.$$

Hemos demostrado el

TEOREMA 3 *La extracción de la raíz de n-ésimo grado del número complejo* $z = |z|(\cos\varphi + i\operatorname{sen}\varphi)$ *siempre es posible. Todos los n valores de la raíz de n-ésimo grado de z, se hallan dispuestos en los vértices del n-ágono regular, inscripto en la circunferencia con centro en el origen y de radio* $\sqrt[n]{|z|}$:

$$\sqrt[n]{z} = \sqrt[n]{|z|}\left(\cos\frac{\varphi+2\pi k}{n} + i\operatorname{sen}\frac{\varphi+2\pi k}{n}\right), \tag{16}$$

$k = 0, 1, \ldots, n-1$.

COROLARIO *Las raíces de n-ésimo grado de* 1, *se expresan por medio de la fórmula*

$$\sqrt[n]{1} = \varepsilon_k = \cos\frac{2\pi k}{n} + i\operatorname{sen}\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1. \tag{17}$$

Ellas se hallan dispuestas en los vértices del n-ágono regular, inscripto en la circunferencia con centro en el origen y de radio 1. ■

De (16) y (17) se aprecia inmediatamente, que $\sqrt[n]{z}$ tendrá cero, una o dos raíces reales, y $\sqrt[n]{1}$, una o dos.

La raíz de n-ésimo grado de 1 se llama *primitiva* (o *prototipo*), si es que ella no es raíz de 1 un grado menor. Tales serán, por ejemplo

$$\varepsilon = \varepsilon_1 = \cos \frac{2\pi}{n} + i \operatorname{sen} \frac{2\pi}{n}, \text{ y } \varepsilon_{n-1}.$$

Cualquier otra raíz ε_k es potencia de una primitiva

$$\varepsilon_k = \varepsilon_1^k,$$

lo que, nuevamente, puede ser apreciado en la fórmula de Moivre. Más aún, $\varepsilon_k \varepsilon_l = \varepsilon_{k+l}$, si se toma $k + l$ por el módulo n. En particular, $\varepsilon_k^{-1} = \varepsilon_{n-k}$, $\varepsilon_0 = 1$. Siendo experimentados en la teoría de grupos, observamos, de este modo, que *las raíces de grado n-ésimo de* 1, *forman el grupo cíclico* $\langle \varepsilon \rangle$ *de orden n.*

Con esto mismo, se obtuvo otra realización más del grupo cíclico de orden n. Por el teorema 6 del § 3 del cap. 4, todos sus subgrupos se encuentran en relación recíprocamente unívoca con el divisor positivo d del número n. Para cada d/n en $\langle \varepsilon \rangle$ se tiene exactamente un subgrupo $\langle \varepsilon^{\frac{n}{\alpha}} \rangle$ de orden d. *La raíz* ε_m *será primitiva si, y sólo si,* $\langle \varepsilon_m \rangle = \langle \varepsilon \rangle$, *o sea, si* Card $\langle \varepsilon^m \rangle = n$, *y esto sólo es posible si m y n son primos entre sí.* Por ejemplo, para $n = 12$, las raíces primitivas serán ε, ε^5, ε^7, ε^{11}. En caso de un primo $n = p$, todas las raíces de la unidad, distintas de 1, son primitivas. Desde el punto de vista algebraico, sin contar la representación geométrica, todas las raíces primitivas del grado n dado, son equivalentes.

Volviendo a la cuestión de la extracción de la raíz de grado n de un número complejo arbitrario $z \neq 0$, observemos, que si z' es alguna raíz dada (digamos, $z' = \sqrt[n]{|z|}\left(\cos \frac{\varphi}{n} + i \operatorname{sen} \frac{\varphi}{n}\right)$, entonces, las restantes raíces tienen la forma $z'\varepsilon_k$, $k = 0, 1, \ldots, \ldots, n - 1$. Esta afirmación se halla en correspondencia con la fórmula (16).

5. Teorema de unicidad. La ventaja del campo C con respecto al $\mathbb{R}$ podremos evaluarla posteriormente en su totalidad, pero el sólo hecho de que C contiene a todas las raíces de 1, justifica el elevado interés hacia los números complejos. Surge la pregunta natural, de cúal es la amplitud de la familia de campos, que poseen propiedades análogas. Resulta, que es legítimo el teorema *siguiente de unicidad del campo de los* números complejos.

TEOREMA 4. *Sean, K, un campo isomorfo a* $\mathbb{R}$ *(en particular,* $K = \mathbb{R}$*), y P la ampliación, obtenida de K por la adjunción de la raíz de la ecuación* $x^2 + 1 = 0$. *Entonces, P es isomorfo a* C.

DEMOSTRACION. Por la definición dada en el punto 5 del § 4 del cap. 4, $P = K(j)$ es el subcampo mínimo de cierto campo F, que contiene a K y j. Como el campo F está dado, podemos considerar los elementos del tipo $a + jb$, con $a, b \in K$, donde el producto

y la adición se comprenden en el sentido de las operaciones definidas en F. A los distintos pares, a, $b \in K$, les corresponden distintos elementos $a + jb$, por cuanto, en caso contrario, se encontraría un elemento nulo $a' + jb'$, con $a' \neq 0$ o $b' \neq 0$. Si $b' = 0$, entonces evidentemente, $a' = 0$. Y si $b' \neq 0$, entonces, obtenemos $j = -a/b' \in K$, lo que es absurdo: $K \cong \mathbb{R}$, y en $\mathbb{R}$ la ecuación $x^2 + 1 = 0$ es irresoluble; por lo tanto, $j \notin K$. Utilizando solamente la igualdad $j^2 = -1$ y operando en el campo F, obtenemos las fórmulas

$$(a_1 + jb_1) + (a_2 + jb^2) = (a_1 + a_2) + j(b_1 + b_2),$$
$$(a_1 + jb_1) \cdot (a_2 + jb^2) = (a_1a_2 - b_1b_2) + j(a_1b_2 + a_2b_1). \quad (18)$$

Además,

$$(a + jb)^{-1} = \frac{a}{a^2 + b^2} + j\frac{-b}{a^2 + b^2} \text{ con } a^2 + b^2 \neq 0.$$

Esto muestra, que el conjunto $\{a + jb \mid a, b \in K\}$, contenido en P, es cerrado con respecto a todas las operaciones en F y, por consiguiente, forma un campo. En virtud de que P es mínimo, tiene lugar la igualdad

$$P = \{a + jb \mid a, b \in K\}.$$

Luego, las fórmulas (18) coinciden con exactitud con las fórmulas (9).

Si $f\colon K \to \mathbb{R}$ es el isomorfismo dado, entonces, la aplicación

$$f^*\colon a + jb \to (f(a), f(b)),$$

que confronta a los elementos del campo P los puntos del plano complejo C con las coordenadas $f(a)$, $f(b)$, será, por lo expresado antes, un isomorfismo de los campos P y C. ∎

Un campo P, contenido en M_2, fue examinado en el punto 1. Pero, tales campos, por supuesto, existen cuantos se quiera (en el parágrafo siguiente se aportará otra construcción más). Según lo demostrado, todos ellos son isomorfos. Observemos, que en la formulación del teorema 4 hubiese correspondido escribir $x^2 + 1 = \tilde{0}$, donde 1, 0, son los elementos unidad y nulo del campo K. Digamos, en el campo $P \subset M_2$, tenemos $J^2 + \tilde{1} = \tilde{0}$, donde $\tilde{1} = E$ y $\tilde{0}$ es la matriz nula.

En el campo C, además de $\mathbb{Q}$ y $\mathbb{R}$, están contenidos muchos otros subcampos. Son particularmente interesantes las ampliaciones del campo $\mathbb{Q}$, que se obtienen al adjuntar un elemento cualquiera de C, no contenido en $\mathbb{Q}$.

EJEMPLO 1 (*campo cuadrático*). Sea d un número entero distinto de cero, que puede ser negativo, y tal que, $\sqrt{d} \notin \mathbb{Q}$. El campo $\mathbb{Q}(\sqrt{d}) \supset \mathbb{C}$ se llama *cuadrático real* para $d > 0$, y campo *cuadrático imaginario* para $d < 0$. Se hizo mención del campo $\mathbb{Q}(\sqrt{2})$ en el § 4 del cap. 4. Un razonamiento que literalmente repite el proceso de demostración del teorema 4, si se sustituye j por

$\sqrt{d}$, y la relación $j^2 = -1$ por $(\sqrt{d})^2 = d$, demuestra que,

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

En particular, las fórmulas (18) se reescriben en la forma

$$\begin{aligned} &(a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{d}, \\ &(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}. \end{aligned} \quad (19)$$

Luego,

$$(a + b\sqrt{d})^{-1} = \frac{a}{a^2 - db^2} + \frac{-b}{a^2 - db^2}\sqrt{d}$$

para $a + b\sqrt{d} \neq 0$ (o sea, cuando a y b no son a un mismo tiempo iguales a cero).

Utilizando (19), es fácil comprobar que la aplicación

$$f\colon a + b\sqrt{d} \mapsto a - b\sqrt{d}$$

es un automorfismo del campo $\mathbb{Q}(\sqrt{d})$ (análogo de conjugación compleja). Se llama *norma* del número $\alpha = a + b\sqrt{d}$, el número

$$N(\alpha) = a^2 - db^2 = \alpha f(\alpha).$$

Evidentemente, $N(\alpha) = 0 \Leftrightarrow \alpha = 0$. Luego, como f es un automorfismo, entonces,

$$N(\alpha\beta) = \alpha\beta f(\alpha\beta) = \alpha\beta f(\alpha) f(\beta) = \alpha f(\alpha)\cdot\beta f(\beta) = N(\alpha)\cdot N(\beta).$$

En particular, $N(\alpha)\cdot N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$. Por eso, la norma posee propiedades esenciales (de cuadratura) del módulo en el campo $\mathbb{C}$.

EJEMPLO 2. (*campo numérico constructivo*). En el plano cartesiano $\mathbb{R}^2$ consideramos dados los puntos (0, 0) y (1, 0). Las construcciones subsiguientes se efectúan solamente con la ayuda de una regla y un compás. Habiendo construido dos puntos P y Q, naturalmente, podemos considerar como construido el segmento PQ que los une. Si se tienen el punto P y el segmento r, también se puede construir la circunferencia de radio r con centro en el punto P. Las intersecciones de par en par de rectas (segmentos) ya trazadas y de circunferencias, son constructivas en el mismo sentido.

El número complejo $a + ib \in \mathbb{C}$ se denomina constructivo, si, con ayuda de una sucesión finita de construcciones (permisibles) como las indicadas más arriba podemos construir, partiendo de (0,0) y (1, 0), el punto $P = (a, b)$. No es difícil observar, que la constructividad de $a + ib$ es equivalente a la constructividad de $|a|$ y $|b|$. El conjunto de los puntos del plano, construidos con ayuda de compás y regla y, en consecuencia, el conjunto de todos los números complejos constructivos, los indicamos con el símbolo CS.

TEOREMA 5. *El conjunto CS es un subcampo del campo $\mathbb{C}$.*

DEMOSTRACIÓN. De la definición de constructividad de los números se deduce inmediatamente el carácter cerrado de CS con respecto a las operaciones de suma y de paso de $z = a + ib \in CS$ a $-z = -a - ib$.

Trazando en los ejes de las coordenadas los segmentos de las líneas constructivas 1, α, β, (fig. 18) y considerando los triángulos semejantes dibujados en los esquemas (constructivos) más abajo (son posibles pequeñas modificaciones), nos convencemos de la

constructividad del producto $\gamma = \alpha\beta$ y del cociente $\delta = \alpha/\beta$. Como las construcciones $zz' = (a + ib)(a' + ib') = (aa' - bb') + i(ab' + a'b)$ y $1/z = a(a^2 + b^2) + ib(a^2 + b^2)$ se reducen, en último análisis, a la construcción de magnitudes del tipo de γ y δ, también queda establecida la constructividad del producto zz' y del

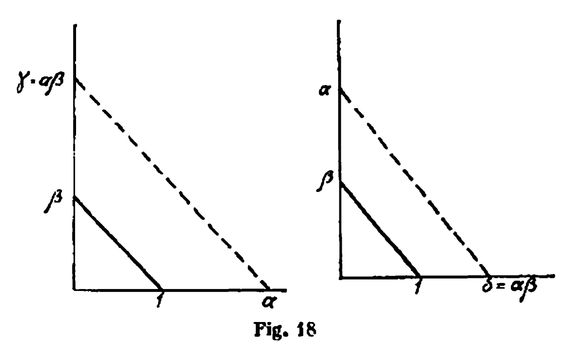


Fig. 18

cociente $1/z$. Al mismo tiempo, queda demostrado el cierre del conjunto CS con respecto a todas las operaciones en el campo $\mathbb{C}$.

A cualquier subcampo $P \subset CS$ se lo suele llamar campo numérico constructivo. Se entiende, que $\mathbb{Q} \subset P$ y que P es un campo de característica nula.

EJERCICIOS

1. Hallar todos los números complejos z, de módulos iguales a 1, para los cuales $z^2 + (1 - i)z$ tiene valores puramente imaginarios. Representar el correspondiente lugar geométrico de los puntos en el plano $\mathbb{C}$.

2. ¿Qué se puede decir del campo $\mathbb{R}(\delta)$, que fue obtenido de $\mathbb{R}$ por adjunción del número complejo δ, que satisface la igualdad $\delta^4 = -1$?

3. Sean, $A, B \in M_n(\mathbb{R})$. Basándose en el teorema 1, demostrar que $\det(A + iB) = \det(A - iB)$ (la raya significa conjugación).

4. Sean, $A, B \in M_n(\mathbb{R})$,

$$C = \begin{Vmatrix} A & -B \\ B & A \end{Vmatrix} \in M_{2n}(\mathbb{R}).$$

Aplicándole a la matriz real C transformaciones elementales de primer y segundo tipo sobre el campo de los números complejos $\mathbb{C}$, demostrar que

$$\det C = |\det(A + iB)|^2.$$

5. (G. Polia y G. Segue). Usando los ejercicios 3 y 4, dar una explicación del «extraño» hecho siguiente. El sistema lineal cuadrado homogéneo

$$d_{11}z_1 + \ldots + d_{1n}z_n = 0,$$
$$\ldots\ldots\ldots\ldots$$
$$d_{n1}z_1 + \ldots + d_{nn}z_n = 0$$

con los coeficientes complejos $d_{kl} = a_{kl} + ib_{kl}$ y las incógnitas $z_l = x_l + iy_l$, tiene una solución no trivial $(z_1, \ldots, z_n)$ con exactitud cuando $\det (d_{kl}) = a + ib = 0$ (véase las observaciones generales sobre esta cuestión en el punto 7 del § 4 del cap. 4). Esta condición lleva a las dos ecuaciones $a = 0$, $b = 0$, que vinculan a $2n^2$ magnitudes reales a_{kl}, b_{kl}. Por otra parte, el sistema (*) puede ser presentado en forma de un sistema de $2n$ ecuaciones lineales homogéneas, con $2n$ incógnitas reales x_l, y_l. Ahora, la condición de solución no trivial, se escribe en forma de igualdad a cero de un determinante real de dimensiones $2n \times 2n$, lo que da sólo una ecuación entre a_{kl}, b_{kl}. ¿Cómo conciliar entre sí estos dos resultados?

6. Teniendo en cuenta, que los automorfismos del campo cuadrático $Q(\sqrt{d})$ deben dejar en su lugar a los números racionales, hallar los automorfismos de este campo. (*Respuesta*. La aplicación unitaria y $a + b\sqrt{d} \to a - b\sqrt{d}$).

7. ¿A qué es igual la suma de todas las raíces de grado $n > 1$, de 1? ¿Qué se puede decir sobre la suma de las raíces primitivas de grado 12 y de grado 15 de 1?

8. Hallar y representar el núcleo geométrico y la imagen de la aplicación $(\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, definida por la correspondencia $t \mapsto e^{2\pi i t}$ (véase la fórmula (15)).

§ 2. ANILLO DE POLINOMIOS

Juntamente con los sistemas lineales, examinados por nosotros en los cap. 2 y 3, los polinomios componen una vieja y bien estudiada sección del álgebra tradicional. En el lenguaje de los polinomios se formulan o se resuelven los más diversos problemas de las matemáticas. Esto se debe a muchas causas, una de las cuales consiste en la propiedad de universalidad del anillo de los polinomios, en la que nos detendremos brevemente en los puntos 1 y 2.

Sean K un anillo conmutativo (y, como de costumbre, asociativo) con la unidad 1, y A cierto subanillo del mismo, contenedor de 1. Si $t \in K$, entonces, el menor subanillo en K, contenedor de A y t, estará, evidentemente, compuesto de elementos del tipo

$$a(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n,$$

donde $a_s \in A$, $n \in \mathbb{Z}$, $n \geqslant 0$. Lo designamos con el símbolo $A[t]$ y lo llamamos anillo obtenido de A con la adjunción del elemento t, y a la expresión (*), la denominamos polinomio de t con coeficientes en A. Qué entender por suma y por producto de polinomios se ve de los sencillísimos ejemplos:

$$a(t) = b(t) = (a_0 + a_1 t + a_2 t^2) + (b_0 + b_1 t + b_2 t^2) = \\ = (a_0 + b_0) + (a_1 + b_1)t + (a_2 + b_2)t^2,$$

$$a(t) \cdot b(t) = a_0 b_0 + (a_0 b_1 + a_1 b_0)t + \\ + (a_0 b_2 + a_1 b_1 + a_2 b_0)t^2 + (a_1 b_2 + a_2 b_1)t^3 + (a_2 b_2)t^4.$$

Evidentemente, la reducción de términos semejantes, se basa en la permutabilidad de dos en dos de todos los elementos a_i, b_j, t^k.

Ahora es el momento propicio para recordar que t es un elemento del anillo K tomado al azar, y, por eso, expresiones (*) exterior-

mente distintas, pueden coincidir de hecho. Si, digamos, $A = \mathbb{Q}$, $t = \sqrt{2}$, entonces $t^2 = 2$ y $t^3 = 2t$, son relaciones que de ningún modo se desprenden de las reglas formales. A fin de llegar al concepto habitual de polinomio, es necesario liberarse de todas las relaciones secundarias semejantes, para lo cual, t debe interpretarse como un símbolo arbitrario, no obligatoriamente contenido en K. El está destinado a jugar un papel puramente auxiliar. Tienen un significado mucho mayor las reglas, de acuerdo a las cuales se forman los coeficientes de las expresiones $a(t) + b(t)$, $a(t)\,b(t)$. Teniendo en cuenta estas observaciones previas, pasamos a la determinación exacta del objeto algebraico denominado polinomio, y de la reunión de tales objetos, llamada anillo de polinomios.

1. Polinomios de una variable. Sea A, un anillo con unidad, conmutativo arbitrario. Construyamos un nuevo anillo B, cuyos elementos son sucesiones ordenadas infinitas

$$f = (f_0, f_1, f_2, \ldots),\ f_i \in A, \tag{1}$$

tales, que todas las f_i, excepto el número finito de las mismas, son iguales a cero. Determinemos en el conjunto B las operaciones de suma y de multiplicación, haciendo

$$f + g = (f_0, f_1, f_2, \ldots) + (g_0, g_1, g_2, \ldots) =$$
$$= (f_0 + g_0, f_1 + g_1, f_2 + g_2, \ldots),$$
$$f \cdot g = h = (h_0, h_1, h_2, \ldots),$$

donde

$$h_k = \sum_{i+j=k} f_i g_j,\ k = 0, 1, 2, \ldots$$

Está claro, que, como resultado de la suma y multiplicación, de nuevo se obtienen sucesiones de la forma (1), con un número finito de términos distintos de cero, o sea, elementos de B. La comprobación de todos los axiomas del anillo (véase el § 4 del cap. 4) excepto, quizás, el axioma de asociatividad, es evidente. Efectivamente, por cuanto la suma de dos elementos de B se reduce a la suma de un número finito de elementos del anillo A, $(B, +)$ resulta un grupo conmutativo con elemento nulo $(0, 0, 0, \ldots)$ y elemento $-f = (-f_0, -f_1, -f_2, \ldots)$, contrario al arbitrario $f = (f_0, f_1, f_2, \ldots)$. Luego, la conmutatividad de la multiplicación, se desprende directamente de la simetría de la expresión de los elementos h_k por medio de f_i y de g_j. Esta misma expresión muestra, que en B se ha cumplido la ley distributiva $(f + g)\,h = fh + gh$. En lo que se refiere a la asociatividad de la operación de multiplicación, sean

$$f = (f_0, f_1, f_2, \ldots),\quad g = (g_0, g_1, g_2, \ldots),\quad h = (h_0, h_1, h_2, \ldots)$$

tres elementos cualesquiera del conjunto B. Entonces, $fg = d =$ $= (d_0, d_1, d_2, \ldots)$, donde $d_l = \sum_{i+j=l} f_i g_j$, $l = 0, 1, 2, \ldots,$ $\ldots$, y $(fg)h = dh = e = (e_0, e_1, e_2, \ldots)$, donde $e_s = \sum_{l+k=s} d_l h_k =$ $= \sum_{l+k=s} \left(\sum_{i+j=l} f_i g_j \right) h_k = \sum_{i+j+k=s} f_i g_j h_k$. El cálculo de $f(gh)$ da el mismo resultado. Así pues, *B es un anillo conmutativo y asociativo con unidad* $(1, 0, 0, \ldots)$.

Las sucesiones $(a, 0, 0, \ldots)$ se suman y se multiplican del mismo modo que los elementos del anillo A. Esto permite identificar tales sucesiones con los elementos correspondientes de A, o sea, hacer $a = (a, 0, 0, \ldots)$ para todas las $a \in A$. De este modo, A se transforma en subanillo del anillo B. Designemos luego $(0, 1, 0, 0, \ldots)$ por X y llamemos a X *variable* (o *incógnita*) sobre A. Utilizando la operación de multiplicación, introducida en B, hallamos que,

$$X = (0, 1, 0, 0, \ldots),$$
$$X^2 = (0, 0, 1, 0, \ldots),$$
$$\cdots\cdots\cdots\cdots$$
$$X^n = (0, 0, \ldots, 0, 1, 0, \ldots).$$

Además, en virtud de (2) y debido a la inclusión $A \subset B$, tenemos

$$(0, 0, \ldots, 0, a, 0, \ldots) = aX^n = X^n a.$$

Así, si f_n es el último término distinto de cero de la sucesión $f =$ $= (f_0, f_1, \ldots, f_n, 0, 0, \ldots)$, entonces, en las nuevas designaciones

$$\begin{aligned} f &= (f_0, \ldots, f_{n-1}, 0, 0, \ldots) + f_n X^n = \\ &= (f_0, \ldots, f_{n-2}, 0, 0, \ldots) + f_{n-1} X^{n-1} + f_n X^n = \\ &= f_0 + f_1 X + f_2 X^2 + \ldots + f_n X^n. \end{aligned} \qquad (3)$$

Esta representación del elemento f es unívoca, por cuanto $f_0, \ldots$ $\ldots, f_n$, en el segundo miembro de (3), son términos de la sucesión $(f_0, \ldots, f_n, 0, \ldots)$, que es igual a cero si, y sólo si, $f_0 = \ldots$ $\ldots = f_n = 0$.

DEFINICION. El anillo B, introducido más arriba, se designa por $A[X]$ y se llama *anillo de polinomios sobre A, de una variable X*, y sus elementos se denominan *polinomios*.

Desde luego, el atributo a la letra fija X, del nombre de variable o de incógnita, no es un hallazgo terminológico muy feliz, pero arraigó, por cuanto no lleva confusión.

Hemos introducido intencionalmente la letra mayúscula X, para diferenciar nuestro polinomio $f = X$, especialmente separado, de la variable teórica-funcional x, que recorre cierto conjunto de valores (un acuerdo puramente temporal, que en el futuro no es obligatorio observar). Es más habitual la escritura del polinomio f en la forma

$$f(X) = a_0 X^n + a_1 X^{n-1} + \ldots + a_n,$$

o sea, en el orden decreciente de las potencias de X. En adelante, lo escribiremos del modo que sea más cómodo. Los elementos f_i (y los a_i) se llaman *coeficientes* del polinomio f. El polinomio f *es nulo*, cuando todos sus coeficientes son iguales a cero. El coeficiente f_0 de X elevado a la potencia cero, también se llama *término constante* o *término independiente*. Si $f_n \neq 0$, entonces, f_n se llaman coeficiente *superior*, y n *grado* del polinomio, y se escribe $n = \deg f$. Al polinomio nulo se le adjudica el grado de $-\infty$ $(-\infty + (-\infty) = -\infty$, $-\infty + n = -\infty$, $-\infty < n$, para cada $n \in \mathbb{N})$. Los polinomios de los grados 1, 2, 3, . . ., se llaman, respectivamente, *lineales*, *cuadrados*, *cúbicos*, etc.

El elemento unitario 1 del anillo A, desempeña el papel de unidad en el anillo $A[X]$, y se considera polinomio de grado nulo. De la definición de las operaciones de adición y de multiplicación en $A[X]$ se deduce directamente que para dos polinomios cualesquiera

$$f = f_0 + f_1X + \ldots + f_nX^n, \quad g = g_0 + g_1X + \ldots + g_mX^m \quad (4)$$

de los grados n y m respectivamente, tienen lugar las desigualdades

$$\deg (f + g) \leqslant \text{máx} (\deg f, \deg g), \quad \deg (fg) \leqslant \deg f + \deg g. \quad (5)$$

La segunda de las desigualdades (5) en realidad se sustituye por la igualdad

$$\deg (fg) = \deg f + \deg g$$

siempre, cuando el producto f_ng_m de los coeficientes superiores de los polinomios (4) es distinto de cero, por cuanto,

$$fg = f_0g_0 + (f_0g_1 + f_1g_0) X + \ldots + (f_ng_m) X^{n+m}. \quad (6)$$

Pero, esto significa, que es cierto el

TEOREMA 1 *Si A es un anillo íntegro, entonces, el anillo $A[X]$ también es íntegro.* ■

El lugar que ocupa el anillo de polinomios dentro de los anillos conmutativos, en parte lo aclara el siguiente

TEOREMA 2 *Sea, que el anillo conmutativo K, contiene A en calidad de subanillo. Para cada elemento $t \in K$ existe un homomorfismo único de los anillos Π_t: $A[X] \to K$,* tal que,

$$\Pi_t (a) = a, \quad \forall a \in A, \quad \Pi_t (X) = t. \quad (7)$$

DEMOSTRACION Supongamos primeramente, que tal homomorfismo Π_t existe. Como $\Pi_t (f_i) = f_i$ para cada coeficiente del polinomio f, escrito en la forma ordinaria (3), y $\Pi_t (X^k) = (\Pi_t (X))^k = t^k$ (propiedad del homomorfismo y la condición (7)), entonces

$$\Pi_t (f) = \Pi_t (f_0 + f_1X + \ldots + f_nX^n) =$$
$$= f_0 + f_1t + \ldots f_nt^n, \quad (8)$$

o sea, $\Pi_t(f)$ está determinado unívocamente y se expresa por la fórmula (8). A la inversa, dando la aplicación Π_t por la fórmula (8), nosotros, evidentemente, cumpliremos la condición (7) y obtendremos el homomorfismo de los anillos. Esto está claro para la aplicación de grupos aditivos de anillos, y, en lo que respecto a la multiplicación, el empleo de Π_t al producto (6), y el uso posterior de la ley (general) de la distributividad, da

$$\Pi_t(fg) = f_0g_0 + (f_0g_1 + f_1g_0)t + \ldots + (f_ng_m)t^{n+m} =$$
$$= \left(\sum_{i=0}^{n} f_it^i\right)\left(\sum_{j=0}^{m} g_jt^j\right) = \Pi_t(f)\cdot\Pi_t(g). \quad \blacksquare$$

El resultado del empleo de la aplicación Π_t, determinada por la fórmula (8), al polinomio $f = f(X)$, se llama sustitución de t en f en lugar de X, o (a duras penas), sencillamente valor de f, para $X = t$, de modo que $\Pi_t(f) = f(t)$. Conocer $\Pi_t(f)$, significa saber calcular el valor de f cuando $X = t$. Los homomorfismos Π_x, $x \in A$, sirven de eslabón de enlace entre los puntos de vista funcional y algebraico sobre el polinomio. Por definición, el polinomio $X - c = (-c, 1, 0, \ldots)$ nunca es igual a cero, pero, la función asociada a él $x \mapsto x - c$ adopta el valor nulo para $x = c$. Otro ejemplo: el polinomio, distinto de cero, $X^2 + X$ con coeficientes del campo F_2 (donde $1 + 1 = 0$), representa la función nula $\tilde{f}$: $F \to F_2$, por cuanto $0^2 + 0 = 0$ y $1^2 + 1 = 0$.

El elemento $t \in K$ se llama *algebraico sobre* A, si $\Pi_t(f) = 0$ para cierto $f \in A[X]$. Y, si Π_t: $A[X] \to K$ es una inclusión isomorfa (monomorfismo), entonces, t es un elemento *transcendente sobre* A. En el caso en que $A = \mathbb{Q}$ y $K = \mathbb{C}$, sencillamente se habla de *números algebraicos* y *truscendentes*. Ejemplos de números trascendentes, son e y π, definidos en el análisis matemático. y ejemplos de números algebraicos son $-\sqrt{2}$, $\sqrt{3}$, $\sqrt{2}$, $+\sqrt{3}$.

Para medir la desviación del anillo $A[t] \subset K$, obtenido al principio de este parágrafo, con respecto al anillo de polinomios $A[X]$, introduzcamos en el núcleo considerado $J_t = \operatorname{Ker}\Pi_t$ del homomorfismo Π_t del teorema 2. De acuerdo con (7), Π_t opera en forma semejante en A, por eso $A \cap J_t = 0$. A propósito, $J_t = 0$, si t es un elemento trascendente sobre A. Según el teorema sobre los homomorfismos para los anillos (teorema 2, punto 4, § 4 del cap. 4):

$$A[t] \cong A[X]/J_t. \tag{9}$$

El isomorfismo (9), hablando propiamente, sirve de expresión de *propiedad universal* del anillo de polinomios $A[X]$. De una forma más completa, la universalidad del anillo de polinomios se aprecia de la siguiente afirmación, generalizadora del teorema 2.

TEOREMA 3. *Sean A y K dos anillos conmutativos arbitrarios; t, un elemento de K, y φ: $A \to K$, un homomorfismo. Entonces, existe,*

además es única, una continuación de φ hasta el homomorfismo φ_t: $A[X] \to K$ del anillo de polinomios $A[X]$ en K, que traslada la variable X a t.

La demostración es una modificación insignificante de la demostración del teorema 2 y se deja al lector en calidad de ejercicio. ∎

2. Polinomios de muchas variables. Si en la situación $A \subset K$, considerada al principio del parágrafo, se toman n elementos cualesquiera $t_1, \ldots t_n \in K$ y se considera en K las intersecciones de todos los subanillos, contenedores de $A, t_1, \ldots, t_n$, entonces, obtendremos el anillo $A[t_1, \ldots, t_n]$. La escritura formal de sus elementos nos sugiere, al igual que en el caso de $n = 1$, la necesidad de poner en uso el anillo de polinomios de n variables. Esto se hace muy sencillamente. Recordemos, que la estructura del anillo $B = A[X]$ incluía al anillo conmutativo arbitrario A con la unidad. Podemos ahora sustituir en nuestra estructura el anillo A por el B y construir el anillo $C = B[Y]$, donde Y es una nueva variable independiente, que desempeña con relación a B, el mismo papel que X con relación a A. Los elementos de C se escriben unívocamente en la forma $\sum b_jY^j$, $b_j \in B$, además, B se identifica con un subanillo en C, precisamente, con el conjunto de elementos $bY^0 = b\cdot 1$. Como, a su vez, $b_j = \sum a_{ij}X^i$ es la escritura unívoca de los elementos $b_j \in B$, entonces, cualquier elemento de C tiene la forma

$$\sum_{i=0}^{k} \sum_{j=0}^{l} a_{ij}X^iY^j, \quad a_{ij} \in A,$$

con esto se sobreentiende (por el sentido de la construcción), que los a_{ij} están permutados con X e Y, y que la variable X está permutada con Y. El anillo C se llama anillo de polinomios sobre A de dos variables independientes (de dos incógnitas) X e Y.

Repitiendo un número suficiente de veces esta construcción, obtenemos *el anillo $A[X_1, \ldots, X_n]$ de los polinomios sobre A de n variables independientes (o incógnitas) $X_1, \ldots, X_n$.*

El conjunto $(i_1, \ldots, i_n) \in \overline{\mathbb{N}}^n$ de n números enteros no negativos $i_1, \ldots, i_n$ ($\overline{\mathbb{N}} = \mathbb{N} \cup \{0\}$) convenimos en designarlo abreviadamente con el símbolo (i). Entonces, cualquier elemento $f \in A[X_1, \ldots$ $\ldots, X_n]$ se escribe en la forma

$$f = \sum_{(i)} a_{(i)}X^{(i)}, \quad a_{(i)} \in A, \tag{10}$$

donde $X^{(i)} = X_1^{i_1} \ldots X_n^{i_n}$ es un *monomio*, así que f es una combinación lineal de monomios con coeficientes de A. En correspondencia con la definición de polinomios, todos los coeficientes $a_{(i)}$ en (10), a excepción de un número finito de ellos, son iguales a cero. La unicidad de la escritura (10) se deduce inmediatamente de la siguiente afirmación.

El polinomio f es igual a cero si, y sólo si, son nulos todos sus coeficientes $a_{i_1} \ldots {}_{i_n}$. Para $n = 1$ esto ya se hizo notar en el curso de la construcción del anillo $A[X]$, y para $n > 1$ lo más fácil es utilizar la inducción en n. Precisamente, podemos escribir

$$f = \sum a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n} = \sum_{i_n} b_{i_n} X_n^{i_n},$$

donde

$$b_{i_n} = \sum_{i_1, \ldots, i_{n-1}} a_{i_1 \ldots i_{n-1} i_n} X_1^{i_1} \ldots X_{n-1}^{i_{n-1}}$$

son polinomios del menor número de variables. La afirmación para $n = 1$ y la suposición de inducción demuestran, que

$$f = 0 \Leftrightarrow b_{i_n} = 0, \quad \forall i_n \Leftrightarrow a_{i_1} \ldots {}_{i_{n-1} i_n} = 0, \quad \forall (i_1, \ldots, i_n).$$

Ahora, es natural considerar dos polinomios $f, g \in A[X_1, \ldots, X_n]$ *iguales*, si coinciden sus coeficientes para los mismos monomios (de acuerdo a lo dicho más arriba $(i_1, \ldots, i_n) \neq (j_1, \ldots, j_n) \Rightarrow X_1^{i_1} \ldots X_n^{i_n} \not\approx X_1^{j_1} \ldots X_n^{j_n}$. Por *grado del polinomio f con relación a X_k*, se entiende el mayor número entero, designado por $\deg_k f$, que se encuentra en calidad de exponente de X_k en $a_{(i)}X^{(i)}$ con $a^{(i)} \neq 0$. Por ejemplo, el polinomio $1 + X + XY^3 + X^2Y^2$ es de grado 2 con respecto a X y de grado 3 con respecto a Y. El número entero $i_1 + \ldots + i_n$ se llama *potencia (total) del monomio $X_1^{i_1} \ldots X_n^{i_n}$. El grado $\deg f$* (o *la potencia total*) *del polinomio f*, será la máxima de las potencias totales de sus monomios. Suponemos $\deg 0 = -\infty$. No tiene sentido hablar del término del polinomio que tiene mayor grado, por cuanto, puede ser que haya varios de esos términos (monomios).

Al anillo $A[X_1, \ldots, X_n]$ se trasladan muchos de los resultados obtenidos por nosotros en el punto 1 para $A[X]$. Por ejemplo, basándonos en el teorema 1 y utilizando la inducción en n, inmediatamente nos convencemos de que es correcto el

TEOREMA 1'. *Si A es un anillo íntegro, entonces, el anillo $A[X_1, \ldots, X_n]$ también es íntegro. En particular, el anillo de los polinomios de n variables sobre cualquier campo P, es de integridad.* ∎

Sea, luego, que A es un subanillo del anillo conmutativo K, y $t_1, \ldots, t_n$, los elementos de K. Entonces, la correspondencia

$$\Pi_{t_1, \ldots, t_n} : f(X_1, \ldots, X_n) \mapsto f(t_1, \ldots, t_n), \quad \forall f \in A[X_1, \ldots, X_n],$$

determina el homomorfismo $A[X_1, \ldots, X_n] \to K$ (comparar con el teorema 2). Con esto se habla de *sustitución de $t_1, \ldots, t_n$ en f*, o del valor de f para $X_1 = t_1, \ldots, X_n = t_n$. Si $\operatorname{Ker} \Pi_{t_1, \ldots, t_n} = 0$, entonces, $t_1, \ldots, t_n$, se denominan *elementos del anillo K algebraicamente independientes sobre A*. En el caso de elementos $t_1, \ldots, t_n$

algebraicamente dependientes, existirá un polinomio no nulo $f \in A[X_1, \ldots, X_n]$, para el cual $f(t_1, \ldots, t_n) = 0$.

Finalmente, al teorema 3 le corresponde el análogo

TEOREMA 3' (de universalidad del anillo de polinomios). *Sean A y K, anillos conmutativos; $t_1, \ldots, t_n$, elementos de K; y, $\varphi: A \to K$, un homomorfismo de los anillos. Entonces, existe una continuación φ hasta el homomorfismo $\varphi_{t_1, \ldots, t_n}: A[X_1, \ldots, X_n] \to K$, que, además, es única y traslada X_i a t_i, $1 \leqslant i \leqslant n$.*

DEMOSTRACION. La misma se efectúa paralelamente a la construcción del propio anillo $A[X_1, \ldots, X_n]$, o sea, por inducción. Basándose en el teorema 3, es natural presuponer que disponemos del homomorfismo $\varphi_{t_1, \ldots, t_{n-1}}: A[X_1, \ldots, X_{n-1}] \to K$, continuador de φ y tal, que $\varphi_{t_1, \ldots, t_{n-1}}(X_i) = t_i$, $1 \leqslant i \leqslant n-1$. Sustituyendo en el teorema 3 el anillo A por $A[X_1, \ldots, X_{n-1}]$, y el homomorfismo φ por $\varphi_{t_1, \ldots, t_{n-1}}$, y aprovechando la circunstancia de que $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$, hallamos el homomorfismo buscado $\varphi_{t_1, \ldots, t_n} = (\varphi_{t_1, \ldots, t_{n-1}})_{t_n}$, que traslada X_n a t_n. La unicidad de $\varphi_{t_1, \ldots, t_n}$ no necesita comprobación, por cuanto $\varphi_{t_1, \ldots, t_n}$ queda totalmente determinada por la operación en A y en los elementos $X_1, \ldots, X_n$, que engendran $A[X_1, \ldots, X_n]$. ∎

COROLARIO. *A cualquier permutación $\pi \in S_n$ que opere en el conjunto $\{1, 2, \ldots, n\}$, le responde el automorfismo, determinado unívocamente, $\tilde{\pi}: f \to \pi f$ del anillo $A[X_1, \ldots, X_n]$, idéntico en A, y tal que,*

$$(\pi f)(X_1, \ldots, X_n) = f(X_{\pi^{-1}(1)}, \ldots, X_{\pi^{-1}(n)}).$$

DEMOSTRACION. Hagamos, en la formulación del teorema 3', $K = A[X_1, \ldots, X_n]$, $t_1 = X_{\pi^{-1}(1)}, \ldots, t_n = X_{\pi^{-1}(n)}$, y tomemos en calidad de φ la limitación de la aplicación idéntica e_K en A. Como resultado, se obtiene el homomorfismo $\tilde{\pi} = \varphi t_1, \ldots t_n$ del anillo $A[X_1, \ldots, X_n]$ en sí mismo (o sea, un endomorfismo) y, como $\tilde{\pi}\widetilde{\pi^{-1}} = \widetilde{\pi^{-1}}\tilde{\pi} = 1$, $1 = \tilde{1}$ y $\tilde{\pi}\tilde{\rho} = \widetilde{\pi\rho}$ (la comprobación fue efectuada en el lema del § 2 del cap. 4), entonces, $\tilde{\pi}$ es un automorfismo.

Sirve de especificación útil del teorema 1', el

TEOREMA 4. *Sean f y g, dos polinomios cualesquiera de n variables sobre el anillo íntegro A. Entonces,*

$$\deg(fg) = \deg f + \deg g.$$

DEMOSTRACION. Denominemos *polinomio homogéneo o forma* de grado m, al polinomio $h(X_1, \ldots, X_n)$, en el que todos los términos tienen una misma potencia total m. Las formas de grados 1, 2, 3, se llaman, respectivamente, formas *lineales*, *cuadráticas* y *cúbicas*.

Uniendo todos los monomios de un mismo grado que *forman parte de* f (o, como también se dice, que *se encuentran, con coeficientes no nulos*), representaremos unívocamente el polinomio $f = \sum a_{(i)}X^{(i)}$ como la suma de varias formas f_m de distintos grados

$$f = f_0 + f^1 + \ldots + f_k, \quad k = \deg f.$$

Si ahora

$$g = g_0 + g_1 + \ldots + g_l, \quad l = \deg g,$$

entonces, evidentemente,

$$fg = f_0g_0 + (f_0g_1 + f_1g_0) + \ldots + f_kg_l$$

(esto se parece a la relación (6), pero, f_i, g_j tienen allí otro sentido), de donde, $\deg fg \leqslant k + l$. Por el teorema 1, de $f_k \neq 0$, $g_l \neq 0$, se desprende que $f_kg_l \neq 0$, o sea, $\deg (fg) = \deg (f_kg_l) = k + l = \deg f + \deg g$. ∎

3. Algoritmo de división con resto. Los anillos de los polinomios de una y de un gran número de variables independientes tienen no solamente propiedades generales, cuidadosamente destacadas por nosotros en el punto 2, sino que también diferencias esenciales. Descubrimos inmediatamente una de estas diferencias, si nos dirigimos a la descripción de los ideales del anillo de los polinomios. Vimos (punto 3 del § 4 del cap. 4), que en el anillo $\mathbb{Z}$ cada ideal es principal, o sea, se expresa como $m\mathbb{Z}$. La demostración de este hecho se basaba en la comparación de números por su magnitud, por medio del mecanismo denominado *algoritmo de división con resto*, ya descrito para $\mathbb{Z}$ en el punto 3 del § 8 del cap. 1. Resulta, que un algoritmo totalmente análogo tiene lugar en el anillo $A[X]$ sobre el anillo íntegro A (para $A = \mathbb{R}$ esto prácticamente es sabido del curso de álgebra elemental: recuerde la operación de división en forma de ángulo).

TEOREMA 5. *Sean A un anillo íntegro, y g un polinomio en $A[X]$ con coeficiente mayor, invertible en A. Entonces, a cada polinomio $f \in A[X]$ se le confronta un, y sólo un, par de polinomios q, $r \in A[X]$, para los cuales*

$$f = qg + r, \quad \deg r < \deg g. \tag{11}$$

DEMOSTRACION. Sean

$$f = a_0X^n + a_1X^{n-1} + \ldots + a_n,$$
$$g = b_0X^m + b_1X^{m-1} + \ldots + b_m,$$

donde $a_0b_0 \neq 0$ y $b_0 \mid 1$. Apliquemos la inducción en n. Si $n = 0$ y $m = \deg g > \deg f = 0$, entonces, hacemos $q = 0$, $r = f$, y si $n = m = 0$, entonces, $r = 0$ y $q = a_0b_0^{-1}$. Supongamos, que el teorema está demostrado para todos los polinomis de grado $< n$ ($n > 0$). Sin limitación de generalidad consideramos a $m \leqslant n$, porque, en el caso contrario, tomamos $q = 0$ y $r = f$. Ya que esto es así,

entonces,

$$f = a_0 b^{-1} X^{n-m} \cdot g + \bar{f},$$

donde $\deg \bar{f} < n$. Por inducción podemos hallar $\bar{q}$ y r, para los cuales $\bar{f} = \bar{q}g + r$, además, $\deg r < m$. Haciendo

$$q = a_0 b^{-1} X^{n-m} g + \bar{q},$$

llegamos al par de polinomios con las propiedades necesarias.

Recurriendo a la propiedad de unicidad del *cociente* q y del *resto* r, suponemos, que

$$qg + r = f = q'g + r'.$$

Entonces, $(q' - q)\, g = r - r'$. Por el teorema 1 tenemos: $\deg (r - r') = \deg (q' - q) + \deg g$, lo que en nuestras condiciones sólo es posible cuando $r' = r$ y $q' = q$ (recordemos, que $\deg 0 = -\infty$ y que $-\infty + m = -\infty$).

Finalmente, los razonamientos expuestos muestran, que los coeficientes del cociente q y del resto r pertenecen al mismo anillo íntegro A, o sea, $f, g \in A[X] \Rightarrow q, r \in A[X]$. ■

OBSERVACION El proceso de la división euclidiana del polinomio f por g se simplifica, si *g es un polinomio unitario*, o sea, si su coeficiente mayor es igual a la unidad. La divisibilidad de f por el polinomio unitario g es equivalente a la igualdad a cero del resto r en la división euclidiana de f por g.

COROLARIO *Todos los ideales del anillo de polinomios $P[X]$ sobre el campo P, son principales.*

DEMOSTRACION Sea T un ideal no nulo cualquiera en $P[X]$. Elegimos el polinomio $t = t(X)$ de grado mínimo, contenido en T. Si f es un polinomio cualquiera de T, entonces, la división con resto por t (P es un campo, por eso no hay necesidad de preocuparse de la inversibilidad del coeficiente mayor de $t(X)$ nos da la igualdad $f = qt + r$, $\deg r < \deg t$. De la misma se deduce, que $r \in T$, por cuanto f, t, qt, son elementos del ideal. En virtud de la elección de t, nos queda por concluir de que $r = 0$. Por consiguiente, $f(X)$ se divide por $t(X)$ y $T = (t) = tP[X]$, o sea, se compone de polinomios divisibles por $t(X)$. ■

En lo que se refiere a los anillos de polinomios de varias variables independientes, entonces, ya en $\mathbb{R}[X, Y]$ a ciencia cierta los ideales no se agotan con los principales.

EJEMPLO. El conjunto

$$T = \{Xf + Yg \mid f, \ g \in \mathbb{R}[X, Y]\},$$

compuesto de polinomios $h(X, Y)$ tales, que $h(0, 0) = 0$, evidentemente, es ideal en $\mathbb{R}[X, Y]$. Como $1 \in \mathbb{R}[X, Y]$, entonces, de $T = t(X, Y)\,\mathbb{R}[X, Y]$ se desprendería la inclusión $t(X, Y) \in T$. Por eso, $t(0, 0) = 0$ y, por lo tanto, $\deg t \geqslant 1$. Aplicando ahora el teorema 4 a las igualdades

$$X = tu, \quad Y = tv,$$

hallaremos que $\deg u = \deg v = 0$, o sea, u, $v \in K$ e $y = u^{-1}vX$ es una contradicción, que muestra que el ideal T no es principal.

El corolario del teorema 5 es cómodo para una descripción clara del isomorfismo (9). En calidad de ejemplo demostremos la afirmación que, en esencia, completa al teorema 4 del § 1.

TEOREMA 6. *El campo de los números complejos* $\mathbb{C}$ *es isomorfo al anillo cociente* $\mathbb{R}[X]/(X^2+1)\mathbb{R}[X]$.

DEMOSTRACIÓN. De acuerdo con (9) $\mathbb{C} = \mathbb{R}[i] \cong \mathbb{R}[X]/J$, donde $J = \{f \in \mathbb{R}[X] \mid f(i) = 0\}$. Puesto que $a + ib \neq 0$ para $(a, b) \neq$ $\neq (0, 0)$, y como $i^2 + 1 = 0 \Rightarrow x^2 + 1 \in J$, entonces, de los razonamientos que demuestran el corolario del teorema 5, sin dificultad se deduce, que $J = (X^2 + 1)\mathbb{R}[X]$.

Las clases adjuntas $(a + bX) + J$; a, $b \in \mathbb{R}$ son los elementos del anillo cociente $\mathbb{R}[X]/J$; la correspondencia $a + ib \mapsto (a+bX) +$ $+ J$ establece el isomorfismo entre $\mathbb{C}$ y $\mathbb{R}[X]/J$. ∎

EJERCICIOS

1. Los polinomios $f(X) = X^5 + 3X^4 + X^3 + 4X^2 - 3X - 1$, $g(X) =$ $= X^2 + X + 1$, pueden ser considerados como pertenecientes al anillo $\mathbb{Z}[X]$ o, digamos, al anillo $\mathbb{Z}_5[X]$, de acuerdo a como se interpreten sus coeficientes. Utilizando el algoritmo de división con resto, mostrar, que en el primer caso $f(X)$ no se divide por $g(X)$, y que en el segundo, se divide. ¿Sería posible realizar la variante opuesta?

2. Demostrar, con ayuda del teorema 3, que, si F es un campo, entonces, el grupo de todos los automorfismos del anillo $F[X]$ es isomorfo al grupo de las transformaciones $X \mapsto aX + b$, donde a, $b \in F$ y $a \neq 0$.

3. Mostrar que el polinomio $f \in F[X_1, \ldots, X_n]$ es una forma de grado m (véase la demostración del teorema 4), si, y sólo si, $f(tX_1, \ldots, tX_n) =$ $= t^m f(X_1, \ldots, X_n)$, donde t es una nueva variable.

4. Mostrar, que el número de distintos polinomios de n variables independientes de potencia total m, es igual a $\binom{m+n-1}{m}$. (*Indicación.* Establecida la relación

$$\sum_{k=0}^{m}\binom{k+s}{k}=\binom{m+s+1}{m},$$

aplicar la inducción en m).

5. Volviendo a las definiciones del punto 1, consideremos el conjunto $A[[X]]$, de las así llamadas *series exponenciales formales* $f(X) = \sum_{i \geqslant 0} a_i X^i$ de variable (incógnita) X, o, si se desea, de la sucesión $(a_0, a_1, a_2, \ldots)$ con cualquier número, posiblemente infinito, de coeficientes $a_i \neq 0$, perteneciente al anillo conmutativo A. Las operaciones con las series exponenciales formales de $A[[X]]$ se efectúan de acuerdo a las mismas reglas que las operaciones con polinomios:

$$\left(\sum a_i X^i\right) + \left(\sum b_i X^i\right) = \sum (a_i + b_i) X^i,$$

$$\left(\sum a_i X^i\right) \cdot \left(\sum b_j X^j\right) = \sum c_k X^k, \quad c_k = \sum_{i+j=k} a_i b_j.$$

Mostrar, que el conjunto $A[[X]]$, considerado junto con estas operaciones, es un anillo asociativo y conmutativo con unidad $1 = (1, 0, 0, \ldots)$.

Como en la serie exponencial $f = \sum a_i X^i$ se incluyen potencias X^i tan grandes como se quieran de la variable X, entonces, en lugar de la potencia deg f, que no tiene ahora sentido, es natural considerar *el orden* $\omega(f)$ que es un número entero, igual al menor índice n, para el cual $a_n \neq 0$ (se supone también que $\omega(0) = +\infty$).

Mostrar, que

(i) $\omega(f+g) \geqslant \min\{\omega(f), \omega(g)\}$. (ii) $\omega(fg) \geqslant \omega(f) + \omega(g)$.

Si A es un anillo íntegro, entonces, $\omega(fg) = \omega(f) + \omega(g)$. En particular, junto con A, el anillo $A[[X]]$ también es íntegro.

Mostrar también, que $A[X]$ es un subanillo en $A[[X]]$.

6. Los polinomios y las series exponenciales se usan frecuentemente en calidad de funciones productoras de distintas magnitudes numéricas. El sentido de la operación con ellas lo explicaremos en dos ejemplos sencillos.

a) Establecer la relación

$$\sum_{i=1}^{k} \binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k},$$

partiendo de la fórmula binomial $\sum \binom{n}{i} X^i = (1+X)^n$ en $Z[X]$ y de la descomposición evidente $(1+X)^m (1+X)^n = (1+X)^{m+n}$.

b) Hallar el número l_n de todas las disposiciones posibles del paréntesis en el producto de longitud n de los elementos de un conjunto con una operación binaria. Con este fin, es cómodo introducir la función productora, o sea, la serie exponencial formal

$$l(X) = \sum_{n \geqslant 1} l_n X^n = X + X^2 + 2X^3 + \ldots,$$

cuyos primeros coeficientes fueron ya calculados en el punto 3 del § 1 del cap. 4. De la evidente relación recurrente

$$l_n = \sum_{k=1}^{n-1} l_k l_{n-k}$$

se desprende, que $l(X)^2 = l(X) - X$. Resolviendo esta ecuación cuadrada hallamos

$$l(X) = \frac{1 - \sqrt{1-4X}}{2}$$

(el signo delante del radical está determinado por la condición $l_n > 0$). Pero, si la serie exponencial $f(X)$ es tal, que $f^r = 1 + \lambda X$, $r \in N$, entonces

$$f(X) = 1 + \sum_{k=1}^{\infty} \left[\prod_{i=0}^{k-1} \left(\frac{1}{r} - i\right)\right] (\lambda X)^k$$

(«desarrollo en la serie de Taylor», que, por ahora, se puede aceptar sin demostración). En nuestro caso $r = 2$, $\lambda = -4$, y una simple sustitución da la expresión fina

$$l_n = \frac{1}{n}\binom{2n-2}{n-1}.$$

Se propone llevar a cabo los cálculos intermedios.

7. El anillo $A[[X, Y]]$ de las series exponenciales formales de dos variables independientes (pero permutables entre sí) X, Y, está compuesto de las expresiones $\sum_{i\geqslant 0,\, j\geqslant 0} a_{ij}X^iY^j$. Comprobar, que

$$B[[Y]] \cong A[[X, Y]] \cong C[[X]],$$

donde $B = A[[X]]$, $C = A[[Y]]$ (repetición de la construcción del anillo de polinomios de muchas variables). Mostrar, que la integridad de A implica la integridad del anillo $A[[X]]$.

§ 3. DESCOMPOSICIÓN EN EL ANILLO DE POLINOMIOS

1. Propiedades elementales de divisibiliad. En distintos lugares, comenzando desde el capítulo 1, tocamos las cuestiones de divisibilidad en el anillo $\mathbb{Z}$ de los números enteros, pero el llamado teorema fundamental de la aritmética nos quedaba, hasta el momento, sin demostrar. Ahora ha llegado el momento de no sólo llenar este hueco, sino también de hacer extensivas las correspondientes afirmaciones a una clase más amplia de anillos. En primer lugar, nos interesa el anillo de polinomios $P[X]$ sobre el campo P.

Comencemos con el anillo íntegro arbitrario K. Los elementos invertibles en K fueron denominados por nosotros divisores de la unidad. Frecuentemente, ellos también se denominan elementos *regulares*. Es completamente evidente, que el polinomio $f \in A[X]$ es invertible (regular) con exactitud, cuando $\deg f = 0$ y $f = f_0$ es un elemento invertible del anillo A, por cuanto $fg = 1 \Rightarrow \deg f + \deg g = \deg 1 = 0$.

Se dice, que el elemento $b \in K$ es divisible por $a \in K$ (o que b es *múltiplo* de a), si existe un elemento $c \in K$ tal, que $b = ac$ (esto se denota $a \mid b$). Si $a \mid b$ y $b \mid a$, entonces, a y b se llaman elementos *asociados*. Entonces, $b = ua$, donde $u \mid 1$. En virtud de la observación hecha más arriba, la asociatividad de los polinomios f, $g \in A[X]$ significa, que ellos se diferencian solamente por el multiplicador invertible de A.

El elemento $p \in K$ se llama *primo* (o *no descomponible*), si p no es invertible y no se puede representar en la forma $p = ab$, donde a, b, son elementos invertibles. En el campo P, cada elemento no nulo es invertible y en P no hay elementos primos. El elemento primo del anillo $A[X]$ más frecuentemente se llama *polinomio irreducible*.

Hagamos notar las siguientes propiedades fundamentales de la relación de divisibilidad en el anillo íntegro K.

1) *Si $a \mid b$, $b \mid c$, entonces*, $a \mid c$. Efectivamente, tenemos $b = ab'$, $c = bc'$, donde b', $c' \in K$. Por eso, $c = (ab')c' = a(b'c')$.

2) *Si $c \mid a$ y $c \mid b$, entonces*, $c \mid (a \pm b)$. Efectivamente, por la condición $a = ca'$, $b = cb'$ para algunos a', $b' \in K$, y en vista de la distributividad de $a \pm b = c(a' \pm b')$.

3) *Si* $a \mid b$, *entonces*, $b \mid bc$. Es claro, que $b = ab' \Rightarrow bc = (ab')\,c = a\,(b\,c)$.

Combinando 2) y 3) obtenemos

4) *Si cada uno de los elementos* $b_1, b_2, \ldots, b_m \in K$ *es divisible por* $a \in K$, *entonces, también será divisible por a el elemento* $b_1c_1 + b_2c_2 + \ldots + b_mc_m$, donde $c_1, c_2, \ldots, c_m$, *son elementos arbitrarios.* ∎

DEFINICIÓN Se dice, que el anillo íntegro *K es un anillo con descomposición univalente en factores primos* (o que *K es un anillo factorial*), si cualquier elemento $a \neq 0$ de K se puede representar en la forma

$$a = up_1p_2 \ldots p_r, \tag{1}$$

donde u es un elemento invertible, y $p_1, p_2, \ldots, p_r$ son elementos primos (no obligatoriamente distintos de dos en dos), además, de la existencia de otra descomposición semejante $a = vq_1q_2 \ldots q_s$ se desprende, que $r = s$, *y*, para una debida numeración de los elementos p_i y q_j será

$$q_1 = u_1p_1, \ldots, q_r = u_rp_r,$$

donde $u_1, \ldots, u_r$, son elementos invertibles.

Admitiendo en la igualdad (1) el valor $r = 0$, aceptamos que los elementos invertibles en K también se descomponen en factores primos. Es claro, que si p es primo y u es un elemento invertible, entonces, el elemento up asociado a p, también es primo. En el anillo $\mathbb{Z}$ con elementos invertibles 1 y -1, la relación del orden ($a < b$) da la posibilidad de separar el número primo *positivo* p, de los elementos primos posibles $\pm p$. En el anillo $P[X]$ es cómodo considerar los polinomios irreducibles *unitarios* (=con coeficiente mayor unitario).

Es legítimo el siguiente general

TEOREMA 1 *Sea K un anillo íntegro cualquiera con descomposición en factores primos. La univocidad de la descomposición en K (factorizabilidad de K) tiene lugar si, y sólo si, cualquier elemento primo* $p \in K$, *divisor del producto* $ab \in K$, *divide, por lo menos, a uno de los factores* a, b.

DEMOSTRACIÓN Sea $ab = pc$. Si

$$a = \prod a_i, \quad b = \prod b_j, \quad c = \prod c_k$$

son descomposiciones de a, b, c en sus factores primos, y K es un anillo con descomposición unívoca, entonces, de la igualdad $\prod a_i \prod b_j = p \prod c_k$ se deduce, que el elemento p es asociado con uno de los a_i o de los b_j, o sea, p divide a a o ab.

Al contrario, establezcamos la univocidad de la descomposición en K, donde $p \mid ab \Rightarrow p \mid a$ o $p \mid b$. Razonando por inducción, supongamos, que la descomposición de todos los elementos de K

con número $\leqslant n$ de factores primos es única (por supuesto, con exactitud de hasta el orden de los factores y de la asociación de éstos). Demostremos ahora esto para cualquier elemento $a \neq 0$, que puede ser descompuesto en $n+1$ factores primos. Precisamente, sean

$$a = \prod_{i=1}^{n+1} p_i = \prod_{j=1}^{m+1} r_j \qquad (2)$$

dos descomposiciones del elemento a con $m \geqslant n$. La condición del teorema, aplicada a $p = p_{n+1}$, nos da, que p_{n+1} debe dividir a uno de los elementos $r_1, \ldots, r_{m+1}$. Sin limitación de generalidad (puesto que esto es cuestión de numeración) consideramos, que $p_{n+1} \mid r_{m+1}$. Pero r_{m+1} es un elemento primo, por eso, $r_{m+1} = up_{n+1}$, donde u, es un elemento invertible. Apoyándose en la ley de simplificación en K (teorema 3 del § 4 del cap. 4), de (2) obtenemos la igualdad $\prod_{i=1}^{n} p_i = u \prod_{j=1}^{m} r_j$. En el primer miembro hay un producto de n factores primos. Por suposición de la inducción $m = n$ y ambas descomposiciones solamente se diferencian en el orden de los elementos primos, provistos, probablemente, de algunos factores invertibles. ∎

En el anillo íntegro arbitrario K, el elemento $a \neq 0$, en general, no está obligado a permitir una descomposición del tipo (1). Lo que es más interesante, es que se tienen anillos íntegros, en los cuales la descomposición en factores primos aunque es posible, no es unívoca, o sea, la condición del teorema 1, que parece trivial, no siempre se cumple.

EJEMPLO. Examinemos el campo cuadrático imaginario $\mathbb{Q}(\sqrt{-5})$ (véase el ejemplo en el punto 5 del § 1), y, en él, el anillo íntegro $K = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. La norma $N(a + b\sqrt{-5}) = a^2 + 5b^2$ de cada elemento distinto de cero $\alpha \in K$, es un número entero positivo. Si α es invertible en K, entonces $N(\alpha)^{-1} = N(\alpha^{-1}) \in \mathbb{Z}$, de donde, $N(\alpha) = 1$. Esto solamente es posible para $b = 0$, $a = \pm 1$. De este modo, en K, al igual que en $\mathbb{Z}$, solamente ± 1 son elementos invertibles. Si $\alpha = \varepsilon\alpha_1\alpha_2 \ldots \alpha_r \neq 0$, $\varepsilon = \pm 1$, entonces, $N(\alpha) = N(\alpha_1) \ldots N(\alpha_r)$. Como $1 < N(\alpha_i) \in \mathbb{N}$, para un α dado, el número de factores r no puede crecer ilimitadamente. Por lo tanto, la descomposición en factores primos en K es posible.

Al mismo tiempo, el número 9 (y no solamente él), permite dos descomposiciones en sus factores primos esencialmente distintas:

$$9 = 3 \cdot 3 = (2 + \sqrt{5})(2 - \sqrt{5}).$$

La no asociatividad de los elementos 3 y $2 \pm \sqrt{-5}$ es evidente. Luego, $N(3) = N(2 \pm \sqrt{-5}) = 9$. Por eso, de la descomposición $\alpha = \alpha_1\alpha_2$ para $\alpha = 3$ ó $2 \pm \sqrt{-5}$ con α_1, α_2 invertibles, resultaría $9 = N(\alpha) = N(\alpha_1) N(\alpha_2)$, o sea, $N(\alpha_i) = 3$, $i = 1, 2$, lo que es imposible, por cuanto la ecuación $x^2 + 5y^2 = 3$ con $x, y \in \mathbb{Z}$ no tiene solución. Con esto queda demostrado que los elementos 3 y $2 \pm \sqrt{-5}$ son primos.

El ejemplo examinado contiene en forma embrionaria un extenso círculo de cuestiones, que parcialmente hasta ahora no han sido resueltas, acerca de los campos cuadráticos $\mathbb{Q}(\sqrt{d})$. El estudio de las mismas forma parte del círculo incumbencias de *la teoría algebraica de los números.*

Antes de establecer, con ayuda del teorema 1, la factorizabilidad de unos u otros anillos, introducimos conceptos auxiliares importantes, que poseen un interés independiente.

2. Máximo común divisor (m. c. d.) y mínimo común múltiplo (mc.m.) en los anillos. Sea K un anillo íntegro. Nosotros entenderemos como *máximo común divisor* (m.c.d.) de dos elementos $a, b \in K$, el elemento $d \in K$, denotado con el símbolo m.c.d. (a, b) y poseedor de dos propiedades:

(i) $d \mid a$, $d \mid b$;

(ii) $c \mid a$, $c \mid b \Rightarrow c \mid d$.

Es claro, que junto con d las propiedades (i), (ii), las tiene cualquier elemento asociado con él. Al contrario, si c y d son dos divisores máximos de los elementos a y b, entonces, tendremos $c \mid d$, $d \mid c$, así que c y d son asociados. La designación m.c.d. (a, b) se refiere a cualquiera de ellos, o sea, en esta escritura los elementos asociados no se destinguen. Teniendo en cuenta tal acuerdo, a las propiedades determinantes (i), (ii) del máximo común divisor se les agregan las siguientes:

(iii) m.c.d. $(a, b) = a \Leftrightarrow a \mid b$;

(iv) m.c.d. $(a, 0) = a$;

(v) m.c.d. $(ta, tb) = t$ m.c.d. (a, b);

(vi) m.c.d. (m.c.d.(a, b), c) = m.c.d. (a, m.c.d. (b, c)).

La comprobación de ellas no representa ninguna dificultad y se le deja al lector. La propiedad (vi) también permite extender el concepto de m.c.d. para cualquier número finito de elementos.

Por analogía con el m.c.d. (a, b), se introduce el concepto dual de *mínimo común múltiplo* $m =$ m.c.m. (a, b) de los elementos $a, b \in K$, también definido con exactitud hasta la asociación, por dos propiedades:

(i′) $a \mid m$, $b \mid m$;

(ii′) $a \mid c$, $b \mid c \Leftrightarrow m \mid c$.

En particular, haciendo $c = ab$, obtenemos, que $m \mid ab$.

TEOREMA 2. *Sea, que para los elementos a, b del anillo íntegro K existen* m.c.d. (a, b) y m.c.m. $((a, b)$. Entonces:

a) m.c.m. $(a, b) = 0 \Leftrightarrow a = 0$ o $b = 0$.

b) $a, b \neq 0$, $m =$ m.c.m. $(a, b) ab = dm \Rightarrow d =$ m.c.d. (a, b).

DEMOSTRACIÓN. La afirmación a) se desprende inmediatamente de la definición de m.c.m. (a, b). Para la demostración de b) nos

es necesario convencernos, de que el elemento d, definido por la igualdad $ab = dm$, posee las propiedades (i), (ii). Efectivamente, $(i') \Rightarrow m = a'a$, $m = b'b$. Entonces $ab = dm = da'a$, de donde, luego de simplificar por a, lo que es permisible en cualquier anillo íntegro, tenemos $b = da'$, o sea $d \mid b$. Análogamente, $ab = dm = db'b \Rightarrow a = db'$, o sea, $d \mid a$. Hemos llegado a (i).

Luego, sean, $a = fa''$, $b = fb''$. Hagamos $c = fa''b''$. Entonces, $c = ab'' = ba''$, es múltiplo común de a y b. De acuerdo con la propiedad (ii'), $c = c'm$ para cierto $c' \in K$, de donde, $fc'm = fc = f^2a''b'' = ab = dm$, o sea, $d = fc'$ y $f \mid d$. Hemos llegado a (ii). ∎

De las propiedades (i), (ii), (i'), (ii') o del teorema 2, no se puede extraer ni el método de cálculo, ni la demostración de la existencia del m.c.d. (a, b) y del m.c.m. (a, b). Por el teorema 2b) solamente se establece la relación entre ellos.

Supongamos ahora por un tiempo, que K es un anillo factorial. Designemos por medio de $\mathcal{P}$ el conjunto de elementos primos en K tal, que cualquier elemento primo de K está asociado con un, y sólo con un, elemento de $\mathcal{P}$. Examinando las descomposiciones de dos elementos $a, b \in K$, es cómodo considerar, que en ellas hay igual cantidad de elementos de $\mathcal{P}$, pero algunos, posiblemente, con indicadores nulos, o sea,

$$a = up_1^{k_1} \dots p_r^{k_r}, \quad b = vp_1^{l_1} \dots p_r^{l_r}, \tag{3}$$
$$u \mid 1, \; v \mid 1; \quad k_i \geqslant 0, \; l_i \geqslant 0; \quad p_i \in \mathcal{P}; \quad 1 \leqslant i \leqslant r.$$

Con ayuda del teorema 1 se obtiene el fácilmente memorizable

INDICIO DE DIVISIBILIDAD. *Sean, a, b, elementos del anillo factorial K, escritos en la forma* (3). *Son legítimas las afirmaciones:*

1) $a \mid b$ *si, y sólo si*, $k_i \leqslant l_i$, $i = 1, 2, \dots, r$;

2) m.c.d. $(a, b) = p_1^{s_1} \dots p_r^{s_r}$, donde $s_i = \min\{k_i, l_i\}$, $i = 1, 2, \dots, r$;

3) m.c.m. $(a, b) = p_1^{t_1} \dots p_r^{t_r}$, *donde* $t_i = \text{máx}\{k_i, l_i\}$, $i = 1, 2, \dots, r$. ∎

De este modo, en calidad de s_i hay que tomar el menor de los dos indicadores k_i, l_i, y en calidad de t_i, al máximo. En particular, los elementos $a, b \in K$ son primos entre sí, o sea, m.c.d. $(a, b) = 1$, exactamente cuando los factores primos que forman parte de la descomposición de uno de los elementos no figuran en la descomposición del otro. El defecto de este indicio de divisibilidad consiste, desde luego, en que en la práctica es muy difícil obtener una descomposición del tipo (3). Aun en el caso en que $K = \mathbb{Z}$ (con esto no se anticipa la factorizabilidad de $\mathbb{Z}$) hay que conformarse con pequeñas variaciones del método de elección directa, de los números primos, menores del número dado n. Es tanto más agradable, que en los anillos factoriales, acerca de los cuales se hablará más abajo, existe una forma efectiva de cálculo del m.c.d. (a, b) y del m.c.m. (a, b).

3. Factorizabilidad de los anillos euclídeos. En algoritmo de la división con resto en $\mathbb{Z}$ y $P(X)$ (véanse el punto 3 del § 8 del cap. 1 y el punto 3 del § 2) hace natural el examen del anillo íntegro K, en el cual a cada elemento $a \neq 0$ se le pone en correspondencia el número entero no negativo
$\delta(a)$, o sea, se define la aplicación

$$\delta: K \setminus \{0\} = K^* \to \mathbb{N} \cup \{0\},$$

de tal modo, que con esto se cumplen las condiciones:

(E1) $\delta(ab) \geqslant \delta(a)$ *para todos los* a, $b \neq 0$ *de* K;

(E2) *Cualesquiera que sean* a, $b \in K$, $b \neq 0$, *se hallarán* q, $r \in K$ (q es «cociente», r es «*resto*»), *para los cuales*

$$a = qb + r; \quad \delta(r) \leqslant \delta(b) \quad \text{o} \quad r = 0. \tag{4}$$

El anillo íntegro K que tiene estas propiedades se llama *anillo euclídeo*. Haciendo $\delta(a) = |a|$ para $a \in \mathbb{Z}$ y $\delta(a) = \deg a$ para $a = a(X) \in P[X]$, llegamos a la conclusión, de que $\mathbb{Z}$ y $P[X]$ son anillos euclídeos.

En los anillos euclídeos existe un procedimiento de determinación m.c.d. (a, b) llamado *algoritmo de división sucesiva* o *algoritmo de Euclides* y que consiste en lo siguiente. Sean dados los elementos no nulos a, b del anillo euclídeo K. Aplicando un número suficientemente grande (pero finito) de veces la prescripción (E2), obtendremos un sistema de igualdades del tipo (4) con el último resto nulo:

$$\begin{array}{ll} a = q_1 b + r_1, & \delta(r_1) < \delta(b) \\ b = q_2 r_1 + r_2, & \delta(r_2) < \delta(r_1), \\ r_1 = q_3 r_2 + r_3, & \delta(_3) < \delta(r_2), \\ \ldots\ldots\ldots\ldots & \\ r_{k-2} = q_k r_{k-1} + r_k, & \delta(r_k) < \delta(r_{k-1}), \\ r_{k-1} = q_{k+1} r_k, & r_{k+1} = 0. \end{array} \tag{5}$$

Esto es efectivamente así, por cuanto la cadena rigurosamente descreciente de los números enteros no negativos $\delta(b) > \delta(r_1) > \delta(r_2) > > \ldots$ debe cortarse, y el corte puede suceder sólo a cuenta de que uno de los restos se reduzca a cero.

Se afirma, que el último resto distinto de cero r_k es precisamente el máximo común divisor de los elementos a y b, en el sentido de la definición dada el punto 2. En realidad, por condición $r_k \mid r_{k-1}$. Avanzando en el sistema (5) de abajo hacia arriba y utilizando la propiedad 4) de la relación de divisibilidad, formulada en el punto 1, obtendremos la cadena $r_k \mid r_{k-1}$, $r_k \mid r_{k-2}, \ldots, r_k \mid r_2$, $r_k \mid r_1$ y, finalmente, $r_k \mid b$, $r_k \mid a$. Por consiguiente, r_k es un divisor común de los elementos a y b. Al contrario, sea c cualquier otro divisor de los mismos elementos. Entonces $c \mid r_1$, y, avanzando ahora en

el sistema (5) de arriba hacia abajo, obtendremos la cadena de relaciones de divisibilidad $c \mid r_2, c \mid r_3, \ldots, c \mid r_k$. La última de ellas nos convence definitivamente, de que el m.c.d. (a, b) existe, al mismo tiempo tiene lugar la igualdad

$$r_k = \text{m.c.d.}\ (a, b). \tag{6}$$

Prestemos luego atención al hecho de que cada resto r_i en el sistema (5) se expresa en forma de combinación lineal con coeficientes en K de los dos restos precedentes r_{i-1} y r_{i-2}. Con esto, r_1 se expresa por medio de a y de b: $r_1 = a - q_1 b$, y r_2 se expresa por medio de b y r_1, con lo que resulta de nuevo una combinación lineal de a y b. La sustitución consecutiva en r_i de las expresiones de r_{i-1} y r_{i-2} por medio de a y b nos da, para $i = k$, la expresión

$$r_k = au + bv \tag{7}$$

con algunos elementos $u, v \in K$.

Confrontando (6) y (7) y tomando en consideración el teorema 2b), obtenemos la siguiente afirmación.

TEOREMA 3. *En el anillo euclídeo K cualesquiera dos elementos a, b tienen máximo común divisor y mínimo común múltiplo. Con ayuda del algoritmo de Euclides se pueden hallar tales $u, v \in K$, que se cumplirá la relación*

$$\text{m.c.d.}\ (a, b) = au + bv.$$

En particular, los elementos $a, b \in K$ son primos entre sí si, y sólo si, existen dos elementos $u, v \in K$, para los cuales

$$au + bv = 1. \ ■$$

COROLARIO. Sean a, b, c, elementos del anillo euclídeo K

(i) *Si* el m.c.d. $(a, b) = 1$ *y* el m.c.d. $(a, c) = 1$, *entonces*, el m.c.d. $(a, bc) = 1$.

(ii) *Si $a \mid bc$ y* el m.c.d. $(a, b) = 1$, *entonces, $a \mid c$.*

(iii) *Si $b \mid a$, $c \mid a$ y* el m.c.d. $(b, c) = 1$, *entonces, $bc \mid a$.*

DEMOSTRACION. (i) De acuerdo al teorema 3, tenemos las igualdades $au_1 + bv_1 = 1$, $au_2 + cv_2 = 1$. Multiplicando ambas igualdades miembro a miembro, obtenemos $a\,(au_1 u_2 + bu_2v_1 + cu_1v_2) + bc\,(v_1v_2) = 1$, que da la necesaria afirmación.

(ii) Tenemos $au + bv = 1$, de donde, $ac \cdot u + (bc)\,v = c$. Pero $bc = aw$, por eso, $c = a\,(cu + wv)$, o sea, $a \mid c$.

(iii) De acuerdo con la propiedad (ii′) del m.c.m.,

$$b \mid a,\ c \mid a \Rightarrow \text{m.c.m.}\ (b, c) \mid a \Rightarrow bc \mid a,$$

por cuanto $bc = $ m.c.d. (b, c) por condición el m.c.m. (b, c) y el m.c.d. (b, c) son iguales a la unidad. ■

El lector fácilmente hará extensiva la afirmación del teorema 3 para el caso de un número arbitrario finito de elementos del anillo euclídeo.

Como paso inmediato para el establecimiento de la factorizabilidad del anillo euclídeo, sirve el

LEMA. *Todo anillo euclídeo K es un anillo con descomposición (o sea, cualquier elemento $a \neq 0$ de K se escribe en la forma (1)).*

DEMOSTRACIÓN. Sea que el elemento $a \in K$ posee un divisor propio b: $a = bc$, donde b y c son elementos no invertibles (en otras palabras, a y b no son asociados). Demostremos, que $\delta(b) < \delta(a)$.

Efectivamente, de acuerdo con (E1), tenemos inmediatamente $\delta(b) \leqslant \delta(bc) = \delta(a)$. Suponiendo el cumplimiento de la igualdad $\delta(b) = \delta(a)$, aprovechamos la condición (E2) y hallamos q, r con $b = qa + r$, donde $\delta(r) < (a)$ o $r = 0$. El caso de $r = 0$, cae en virtud de la no asociatividad de a y b. Por la misma razón $1 - qc \neq 0$. Por consiguiente, nuevamente según (E2) (con la sustitución de a por b), tenemos que

$$\delta(a) = \delta(b) \leqslant \delta(b(1 - qc)) = \delta(b - qa) = \delta(r) < \delta(a)$$

es una contradicción. Y bien, $\delta(b) < (a)$.

Si ahora $a = a_1a_2 \ldots a_n$, donde todos los a_i son invertibles, entonces, $a_{m+1}a_{m+2} \ldots a_n$ es divisor propio de $a_m a_{m+1} \ldots a_n$, y, por lo demostrado,

$$\delta(a) = \delta(a_1a_2 \ldots a_n) > \delta(a_2 \ldots a_n) > \ldots > \delta(a_n) > \delta(1).$$

Esta cadena rigurosamente decreciente de números enteros no negativos tiene una longitud de $n \leqslant \delta(a)$. En consecuencia, se tiene la descomposición máxima de a en sus factores primos. ∎

TEOREMA 4. *Todo anillo euclídeo K es factorial (= K posee la propiedad de descomposición unívoca en sus factores primos).*

DEMOSTRACIÓN. Teniendo en cuenta el lema y el criterio de factorizabilidad, contenido en el teorema 1, nos queda por mostrar, que si p es un elemento primo del anillo K, divisor del producto bc de algunos elementos $b, c \in K$, entonces, p divide bien a b, bien a c.

Efectivamente, cuando $b = 0$ o $c = 0$ no hay nada que demostrar. Y si $bc \neq 0$ y $d =$ m.c.d. (b, p), entonces, d al ser divisor del elemento primo p, bien es igual a 1 (más exactamente, es divisor de 1), bien es asociado con p. En el primer caso b y p resultan primos entre sí, y la afirmación (ii) del corolario del teorema 3 permite concluir, que $p \mid c$. En el segundo caso $d = up$, $u \mid 1$ y, en consecuencia, $p \mid b$. ∎

COROLARIO. *Los anillos $\mathbb{Z}$ y $P[X]$ son factoriales (P es un campo arbitrario).*

La factorizabilidad del anillo de polinomios $P[X_1, \ldots, X_n]$, $n > 1$, que ya no es euclídeo, se establece en el cap. 9. Allí también se ponen ejemplos complementarios de anillos euclídeos.

4. Polinomios irreducibles. Especializando la definición dada antes de elemento primo, subrayamos una vez más, que el polinomio f de grado no nulo del anillo $P[X]$, se llama irreductible en $P[x]$ (o irreducible sobre el campo P), si él no es divisible por nin-

gún polinomio $g \in P[X]$, en el que $0 < \deg g < \deg f$. En particular, todo polinomio de primer grado es irreducible. Es totalmente evidente, que la irreducibilidad del polinomio de orden > 1 o su descomposición en factores irreducibles, son conceptos íntimamente ligados con el campo básico P, como lo muestra el polinomio ya conocido por nosotros de la construcción de números complejos, $X^2 + 1 = (X + i)(X - i)$. El polinomio $X^4 + 4$ es reducible sobre $\mathbb{Q}$, aunque esto no es fácil de adivinar:

$$X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2).$$

Ambos multiplicadores del segundo miembro son irreducibles no sólo sobre $\mathbb{Q}$, sino que también sobre $\mathbb{R}$, siendo reducibles, sin embargo, sobre $\mathbb{C}$.

Tanto los números primos en $\mathbb{Z}$ (véase el § 8 del cap. 4), como los *polinomios irreducibles unitarios* (o sea, *con coeficientes mayores* 1) *sobre el campo arbitrario* P, *son infinitamente muchos.*

En el caso de un campo P infinito esto es claro: es suficiente considerar los polinomios irreducibles del tipo $X - c$, $c \in P$.

Pero si el campo P es finito, entonces sirve el razonamiento de Euclides. Precisamente, sea que ya fueron hallados n polinomios irreducibles $p_1, \ldots, p_n$. El polinomio $f = p_1 p_2 \ldots p_n + 1$ tiene por lo menos un divisor unitario primo, por cuanto $\deg f \geqslant n$. Designemos al mismo por medio de p_{n+1}. El es distinto de $p_1, \ldots$ $\ldots, p_n$, por cuanto, de $p_{n+1} = p_s$ para cierto $s \leqslant n$, se derivaría que $p_s \mid (f - p_1 \ldots, p_n$, o sea, $p_s \mid 1$. ■

Como los polinomios de un grado dado sobre un campo finito, son un número finito entonces, se puede hacer la siguiente conclusión útil.

Sobre cualquier campo finito existen polinomios irreducibles de grados tan grandes como se quiera. ■

Esta afirmación de carácter cualitativo se hará más precisa en el cap. 9.

Los polinomios irreducibles sobre el campo $\mathbb{Q}$ juegan un papel especial en la teoría de los campos de números algebraicos. Como, al multiplicar por el número natural conveniente, siempre se puede pasar de un polinomio de $\mathbb{Q}[X]$ a un polinomio de $\mathbb{Z}[X]$, es natural precisar primeramente la vinculación entre las propiedades de reducción sobre $\mathbb{Q}$ y sobre $\mathbb{Z}$. Teniendo en cuenta otras aplicaciones, demostraremos una afirmación general sobre los polinomios sobre el anillo factorial K. Llamemos *contenido del polinomio* $f = a_0 + a_1 X + \ldots + a_n X^n \in K[X]$, al máximo común divisor $d = d(f)$ de todos sus coeficientes. Hasta ahora, hablábamos de m.c.d. (a, b) de dos elementos, pero las propiedades (i) — (vi) del m.c.d. permiten sin esfuerzo hacer extensivo este concepto a cualquier número finito de elementos de un ainllo íntegro. Si $d(f)$ es un

elemento invertible en K, entonces, el polinomio f se llama *primitivo*.

LEMA DE GAUSS. *Sean, K, un anillo factorial,* y f, $g \in K[X]$. Entonces,

$$d(fg) \approx d(f) \cdot d(g).$$

En particular, el producto de dos polinomios primitivos de nuevo resultará un primitivo (aquí y en lo sucesivo la igualdada se entiende con exactitud hasta la asociatividad).

DEMOSTRACION. Comencemos por la última afirmación. Sean

$$f = a_0 + a_1X + \ldots + a_nX^n,$$
$$g = b_0 + b_1X + \ldots + b_mX^m$$

polinomios primitivos de $K[X]$, el producto fg de los cuales, no es primitivo. Existe, por consiguiente, un elemento primo $p \in K$, que divide a $d(fg)$. Elijamos los menores índices s, t, para los cuales $p \nmid a_s$, $p \nmid b_t$. Tales índices existen en virtud de que f y g son primitivos. El coeficiente de X^{s+t} en fg será

$$c_{s+t} = a_sb_t + (a_{s+1}b_{t-1} + a_{s+2}b_{t-2}) + (a_{s-1}b_{t+1} + a_{s-2}b_{t+2} + \ldots)$$

Como a_{s-i} y b_{t-i} para $i > 0$ se dividen por p por condición y $p \mid c_{s+t}$ por suposición, entonces, tenemos la relación

$$pu = a_sb_t + pv,$$

de la cual se sigue, que $p \mid a_sb_t$. En virtud de la factorizabilidad de K tenemos $p \mid a_s$ o $p \mid b_t$, lo que es una contradicción, que demuestra nuestra afirmación.

Pasando al caso general, escribiremos los polinomios arbitrarios f, $g \in K[X]$ en la forma

$$f = d(f)\, f_0, \quad g = d(g)\, g_0,$$

donde f_0, g_0, son polinomios primitivos. Como $fg = d(f)\, d(g) \cdot f_0g_0$ y, de acuerdo con lo demostrado, $d(f_0g_0) \approx 1$, entonces, pues, $d(fg) \approx d(f)\, d(g)$. ∎

COROLARIO. *El polinomio $f \in \mathbb{Z}[X]$, irreducible sobre $\mathbb{Z}$, sigue siendo también irreducible sobre $\mathbb{Q}$* ($\deg f > 0$).

DEMOSTRACION. De acuerdo con el corolario del teorema 4, $\mathbb{Z}$ es un anillo factorial, por eso, el lema de Gauss es aplicable a $\mathbb{Z}[X]$. Supongamos, que $f = gh$, donde $f \in \mathbb{Z}[X]$, y g, $h \in \mathbb{Z}[X]$. Multiplicando ambos miembros de esta igualdad por el mínimo común múltiplo de los denominadores de todos los coeficientes de g y de h, la escribimos de nuevo en la forma $af = bg_0h_0$, donde a, $b \in Z$ y g_0, h_0, son polinomios primitivos sobre $\mathbb{Z}$. Según el lema de Gauss $ad(f) = b$ (es este caso sin limitación de la generalidad la asociatividad se sustituye por la igualdad), así que se obtiene la descomposición $f = d(f)$, g_0h_0 sobre $\mathbb{Z}$. Queda por recordar la irreducibilidad de f en $\mathbb{Z}[X]$. ∎

CRITERIOS DE IRREDUCIBILIDAD (de Eizenshtein). *Sea*

$$f(X) = X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in \mathbb{Z}[X]$$

un polinomio unitario sobre $\mathbb{Z}$, *cuyos coeficientes* $a_1, \ldots, a_n$ *son divisibles por cierto número primo p, pero* a_n *no es divisible por* p^2. *Entonces,* $f(X)$ *es irreducible sobre* $\mathbb{Q}$.

Efectivamente, presuponiendo lo contrario y utilizando el corolario del lema de Gauss, escribimos f en forma de producto de dos polinomios unitarios sobre $\mathbb{Z}$:

$$f(X) = (X^s + b_1X^{s-1} + \ldots + b_s)(X^t + c_1X^{t-1} + \ldots + c_t), \quad st > 0,$$

esta descomposición también se conserva en el anillo cociente $\mathbb{Z}[X](p) \cong \mathbb{Z}_p[X]$, cuyos elementos se obtienen de los polinomios enteros, tomando sus coeficientes por módulo p. Por condición $\bar{a}_i = \bar{0}$, donde $\bar{a}_i$ es una clase de restos por módulo p, correspondientes al número entero a_i. Pero el anillo $\mathbb{Z}_p[X]$ es factorial (corolario del teorema 4). Comparando dos descomposiciones:

$$X^sX^t = (X^s + \bar{b}_1X^{s-1} + \ldots)(X^t + \bar{c}_1X^{t-1} + \ldots), \quad s + t = n,$$

inevitablemente llegamos a la conclusión, de que $\bar{b}_i = \bar{0} = \bar{c}_j$, o sea que todos los coeficientes b_i c_j, se dividen por p. En este caso, $a_n = b_sc_t$ divisible por p^2 es una contradicción, que establece la legitimidad del criterio de Eizenshtein. ■

OBSERVACION. El criterio opera también en el caso en que el coeficiente superior a_0 es distinto de 1, pero no se divide por p.

EJEMPLO. *El polinomio* $f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ *es irreducible sobre Q para cualquier p primo*

Es suficiente observar, que la cuestión de la irreducibilidad de $f(X)$ es equivalente a la cuestión de la irreducibilidad del polinomio

$$f(X+1) = \frac{(X+1)^p - 1}{(X+1)-1} = X^{p-1} + \binom{p}{1}X^{p-2} + \ldots + \binom{p}{p-2}X + \binom{p}{p-1},$$

cuyos coeficientes, a excepción del mayor, son divisibles por p a la potencia uno (propiedad de los coeficientes binomiales, mencionada en el ejercicio 8 del § 4 del cap. 4) y al cual, en consecuencia, le es aplicable el criterio de Eizenshtein. ■

EJERCICIOS

1. Mostrar, que

$$n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}\cdot\text{m.c.d.}(n, m).$$
$$n\mathbb{Z} \cap m\mathbb{Z} = \mathbb{Z}\cdot\text{m.c.m.}(n, m).$$

2. Sean f, g, polinomios unitarios de $\mathbb{Z}[X]$. Mostrar, que en la expresión m.c.d. $(f, g) = fu + gv$, con $u, v, \in \mathbb{Z}[X]$ se puede considerar $\deg u < \deg g$, $\deg v < \deg f$.

3. ¿Son o no factoriales los anillos $\mathbb{Z}[\sqrt{-3}]$ y $\mathbb{Z}_8[X]$?

4. Descomponer en factores irreducibles en $\mathbb{Z}[X]$ los polinomios $X^n - 1$ para $5 \leqslant n \leqslant 12$.

5. Demostrar, que los factores irreducibles del polinomio homogéneo

$$f(X, Y) = a_0X^n + a_1X^{n-1}Y + \ldots + a_{n-1}XY^{n-1} + a_nY^n \in \mathbb{Q}[X, Y]$$

son homogéneos y que $f(X, Y)$ es irreducible si, y sólo si, es irreducible el polinomio $f(X, 1) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in \mathbb{Q}[X]$.

6. Sean, P un campo y $f(X) = \sum_{i\geqslant 0} t_{a_i} X$ una serie exponencial formal en $P[[X]]$ (véase el ejercicio 5 del § 2). La condición $a_0 \neq 0$, o, lo que es equivalente, $\omega(f) = 0$, es necesaria y suficiente para la existencia de la serie exponencial $g(X) \in P[[X]]$, inversa de f: $fg = 1$. Por ejemplo, $(1 - X)^{-1} = \sum_{i\geqslant 0} X^i$. Con exactitud hasta la asociatividad, X es el único elemento primo en $P[[X]]$. El anillo $P[[X]]$ es factorial. Fundamentar estas afirmaciones.

7. Mostrar, que el $\det(x_{ij}) = \sum_{\pi\in S_n} \varepsilon_\pi x_{\pi(1),1} \ldots x_{\pi(n),n}$ es un plinomio homogéneo irreducible de grado n de n^2 variables independientes x_{ij}. (*Indicación*. Razonando a la inversa, suponer que $\det(x_{ij}) = g_1(\ldots, x_{ij}, \ldots) \times$ $\times g_2(\ldots, x_{ij}, \ldots)$. Como $\det(x_{ij})$ es un polinomio lineal homogéneo de variables que se encuentran en una columna dada, entonces, uno de los factores g_1, g_2, es polinomio lineal homogéneo de x_{ij}, $1 \leqslant i \leqslant n$, para j dado, al mismo tiempo que el otro factor no depende en absoluto de x_{ij}, $1 \leqslant j \leqslant n$. Razonamientos análogos se efectúan al reemplazar las columnas por filas. Sea, digamos, que x_{11} pertenece a g_1. Entonces, g_2 no contiene a x_{1j}, $1 \leqslant j \leqslant n$, de donde se deduce, que g_2 no contiene a x_{ij}, $1 \leqslant i, j \leqslant n$, o sea, que g_2 es una constante).

§ 4. CAMPO DE RELACIONES

1. Construcción del campo de relaciones de un anillo íntegro. En los dos parágrafos precedentes fueron establecidas muchas propiedades, comunes para $\mathbb{Z}$ y $P[X]$. Nuestra finalidad inmediata, es incluir $P[X]$ en un campo, además, esto se debe hacer de la manera, más económica, para la cual puede servir de modelo la inclusión de $\mathbb{Z}$ en $\mathbb{Q}$. De hecho, no es en nada más difícil resolver el mismo problema para un anillo íntegro arbitrario A.

Examinemos el conjunto $A \times A^*$ ($A^* = A \setminus \{0\}$) de todos los pares (a, b) de elementos $a, b \in A$ con $b \neq 0$. Este conjunto lo dividimos en clases, haciendo pares (a, b) y (c, d) pertenecientes a una misma clase, solamente como $ad = bc$; en la escritura: $(a, b) \sim$ $\sim (c, d)$. Es claro, que siempre $(a, b) \sim (a, b)$. Luego, $(a, b) \sim$ $\sim (c, d) \Leftrightarrow (c, d) \sim (a, b)$ y, finalmente, $(a, b) \sim (c, d)$, $(c, d) \sim$ $\sim (e, f) \Leftrightarrow (a, b) \sim (e, f)$. Efectivamente, tienen lugar las igualdades $ad = bc$, $cf = de$, de donde $adf = bcf = bde$, o sea $d(af - be) =$ $= 0$. Pero $d \neq 0$, y en virtud de la integridad del anillo A obtenemos $af = be$, lo que significa $(a, b) \sim (e, f)$. Y bien, la relación $\sim$ es reflexiva, simétrica y transitiva, o sea (véase el § 6 del cap. 1), es una relación de equivalencia en el conjunto $A \times A^*$ y, en consecuencia, determina la división de $A \times A^*$ en clases disjuntas.

Sea $Q(A)$ el conjunto de todas las clases de equivalencia o, lo que es lo mismo, $Q(A)$ es el conjunto cociente $A \times A^*/\sim$ del conjunto $A \times A^*$ por relación de equivalencia $\sim$. Designaremos con el símbolo $[a, b]$ la clase, en la cual se encuentra el par ordenado (a, b). Por definición

$$[a, b] = [c, d] \Leftrightarrow ad = bc. \qquad (1)$$

Si en el conjunto $A \times A^*$ se plantean las operaciones de suma y mutiplicación por medio de las fórmulas

$$(a, b) + (c, d) = (ad + bc, bd); \quad (a, b)(c, d) = (ac, bd)$$

(y esto es posible, por cuanto en A de $b \neq 0$, $d \neq 0$, se sigue $bd \neq 0$), entonces, estas operaciones binarias pueden trasladarse a $Q(A)$ Efectivamente, debemos mostrar, que

$$(a', b') \sim (a, b) \Rightarrow \begin{cases} (a, b) + (c, d) \sim (a', b') + (c, d), \\ (a, b)\cdot(c, d) \sim (a', b')\cdot(c, d). \end{cases}$$

Lo mismo se expresa por medio de las relaciones

$$(ad + bc)\, b'd = (a'd + b'c)\, bd,$$
$$ac\cdot b'd = a'c\cdot bd,$$

la veracidad de las cuales se desprende directamente de la condición $a'b = ab'$. Un resultado análogo obtendremos, sustituyendo (c, d) por (c', d'), donde $cd' = c'd$. Llegamos a la conclusión de que en $Q(A)$ las operaciones de suma y multiplicación, que no dependen de la elección de los representantes en las clases de equivalencia, serán

$$[a, b] + [c, d] = [ad + bc, bd]; \quad [a, b]\,[c, d] = [ac, bd]. \qquad (2)$$

Aquí hubiese sido necesario escribir $[a, b] \oplus [c, d]$ y $[a, b] \odot [c, d]$, pero, sin pérdida de claridad, $\oplus$ y $\odot$ han sido reemplazados por los signos comunes de suma y multiplicación.

Convenzámonos ahora, de que $Q(A)$, examinado junto con las operaciones de (2), es un campo. Efectivamente, por ejemplo, de las relaciones

$$[a, b] + ([c, d] + [e, f]) = [a, b] + [cf + de, df] =$$
$$= [adf + bcf + bde, bdf],$$
$$([a, b] + [c, d]) + [e, f] = [ad + bc, bd] + [e, f] =$$
$$= [adf + bcf + bde, bdf]$$

e deduce la ley de asociatividad para la operación de suma. La asociatividad de la multiplicación es evidente. Luego, las relaciones

$$([a, b] + [c, d])\cdot[e, f] = [ade + bce, bdf],$$
$$[a, b]\,[e, f] + [c, d]\,[e, f] = [adef + bcef, bfdf] =$$
$$= [(ade + bce)\, f, (bdf)\, f]$$

y las condiciones (1) de igualdad de las clases de equivalencia muestran, que se cumple la ley de distributividad. Con la misma facilidad se comprueba la conmutatividad de las operaciones de suma y multiplicación. Para la suma, el cero es $[0, 1]$ ($[0, 1] + [a, b] = [a, b]$), y la unidad para la multiplicación es $[1, 1]$. Luego, $= [a, b] = [-a, b]$, por cuanto, $[a, b] + [-a, b] = [0, b^2] = [0, 1]$. Todo esto, tomado conjuntamente, significa que $Q(A)$ es un anillo conmutativo con unidad. Si $[a, b] \neq [0, 1]$, entonces, $a \neq 0$ en A, por consiguiente, $[b, a] \in Q(A)$ y $[a, b][b, a] = [1, 1]$, así que de multiplicativo inverso de $[a, b] \neq [0, 1]$ sirve $[b, a]$. Así pues, se ha mostrado que $Q(A)$ es un campo.

La comparación $a \mapsto [a, 1]$ define la aplicación inyectiva $f: A \to Q(A)$, que de hecho es un (mono) morfismo de los anillos ($f(a + b) = f(a) + f(b)$, $f(ab) = f(a) f(b)$; $a \neq b \Rightarrow f(a) \neq f(b)$). Para cualquier elemento $x = [a, b] \in Q(A)$, tenemos

$$[b, 1]\, x = [a, 1],$$

así que x es la «relación» $f(a)/f(b)$ de los elementos de $f(A)$. Por esta causa, $Q(A)$ se llama *campo de relaciones* del anillo A.

Es cómodo identificar a cada elemento $a \in A$ con su imagen $f(a) = [a, 1] \in Q(A)$, o sea, sustituir A por $f(A)$. Se puede proceder de un modo un poco distinto: sustituir cada uno de los elementos $[a, 1] \in Q(A)$ por los $a \in A$, sin cambiar todos los restantes elementos del campo $Q(A)$, y realizar los cambios correspondientes en las fórmulas (2). Precisamente, corresponde hacer

$$a + [b, c] = [ac + b, c]; \quad a[b, c] = [ab, c].$$

En consecuencia, el anillo íntegro A, desde un principio resultará ser un subanillo de un campo isomorfo a $Q(A)$ y expresado habitualmente con el mismo símbolo $Q(A)$. Luego de tal identificación, es razonable llamar a los elementos $[a, b]$ *fracciones*, y escribirlos brevemente y en la forma acostumbrada

$$[a, b] = \frac{a}{b}.$$

Las reglas de operaciones con las clases $[a, b]$, introducidas más arriba, repiten, de lo que no es difícil darse cuenta, las reglas de operaciones con fracciones en un campo (véase (10) en el punto 5 del § 4 del cap. 4). Ha sido demostrado por nosotros el

TEOREMA 1 *Para cada anillo íntegro A existe un campo de relaciones (o un campo de cocientes, campo de fracciones) $Q(A)$, cuyos elementos tienen la forma a/b, $a \in A$, $0 \neq b \in A$. Las operaciones con fracciones se someten a las reglas* (1), (2), *donde corresponde hacer* $[a, b] = a/b$. ∎

La construcción de los campos de relaciones se usa en las matemáticas con suficiente frecuencia. Su naturalidad se justifica, aunque más no sea, porque el campo $\mathbb{Q}$ no es otra cosa más que un campo de

relaciones $\mathbb{Q}$ ($\mathbb{Z}$) del anillo $\mathbb{Z}$. Es fácil ver (¡compruebe esto!), que $Q(A) \cong A$, si A es un campo.

OBSEVACION. Se puede demostrar, que si el anillo íntegro A es un subanillo en P, en el cual cada elemento x se escribe en forma de relación a/b de los elementos $a \in A$, $0 \neq b \in A$, entonces, $P \cong \cong Q(A)$. Por ejemplo, $\mathbb{Q}(\sqrt{d}) = Q(\mathbb{Z}[\sqrt{d}])$.

2. Campo de fracciones racionales. Sean P un campo, y P [X] el anillo de polinomios sobre P. El campo de relaciones Q (P [X]) del anillo $P[X]$ se denota con el símbolo $P(X)$ (reemplazando los corchetes por paréntisis) y se llama *campo de fracciones racionales* de la variable X con coeficientes en P.

Cabe hacer notar, que el campo de fracciones racionales $P(X)$ siempre contiene un número infinito de elementos, y que su característica siempre coincide con la del campo P. El campo $\mathbf{F}_p(X)$ brinda un ejemplo de campo infinito de característica $p > 0$.

Cada fracción racional del campo $P(X)$ se escribe (además, de distintas maneras) en forma de f/g (o $\frac{f}{g}$, si no se tiende a una economía de papel), donde f, g, son polinomios del anillo $P[X]$, $g \neq 0$. Por definición, $f/g = f_1/g_1 \Leftrightarrow fg_1 = f_1g$. Es corriente llamar a f *numerador*, y a g *denominador* de la fracción f/g. La fracción no varía, si su denominador y numerador se multiplican por un mismo polinomio no nulo, o se simplifican por cualquier factor común. En particular, el número entero (positivo o negativo) $\deg f - \deg g$, no depende de la representación de la fracción racional no nula en forma de relación (de cociente) f/g de dos polinomios. Este número se llama *grado de la fracción*. Una fracción racional de la variable X se llama *irreducible*, si su numerador y su denominador son primos entre sí. Con exactitud hasta un factor de P, común para el numerador y el denominador, cualquier fracción racional f/g se determina unívocamente por medio de cierta fracción irreducible. En efecto, la división de f y g por el m.c.d. (f, g), conduce a una fracción irreducible, y la igualdad $f/g = f_1g_1$ de dos fracciones irreducibles, expresada en la forma $fg_1 = f_1g$ da $f = cf_1$, $c \in P$, $g = cg_1$ (utilizar el corolario del teorema 4 del § 3).

Si $\deg(f/g) = \deg f - \deg g < 0$, entonces, la fracción (irreducible) f/g se llama *propia* (el polinomio nulo se incorpora a las fracciones propias, por cuanto hemos convenido en considerar $\deg 0 = -\infty$).

TEOREMA 2. *Cada fracción racional de $P(X)$ es unívocamente expresable en forma de la suma de un polinomio y de una fracción propia.*

DEMOSTRACION. El algoritmo de la división con resto, aplicado al numerador y al denominador de la fracción f/g, da la igualdad $f = qg + r$, donde $\deg r < \deg g$. Ahora, $f/g = q + r/g$ es la escritura buscada, la comparación de la cual con cualquier otra expresión

del mismo tipo $f/g = \bar{q} + \bar{r}/\bar{g}$ ($\bar{q}$, $\bar{r}$, $\bar{g} \in P[X]$, $\deg \bar{r} < \deg \bar{g}$) conduce a la relación

$$q - \bar{q} = r/g - \bar{r}/\bar{g} = (r\bar{g} - \bar{r}g)/g\bar{g}.$$

Dado que $q - \bar{q} \in P[X]$, y

$$\deg((r\bar{g} - \bar{r}g)/g\bar{g}) = \deg(r\bar{g} - \bar{r}g) - \deg g - \deg \bar{g} < 0,$$

entonces, esto es posible sólo en el caso en que $q - \bar{q} = 0$ y $r/g = \bar{r}/\bar{g}$. ∎

3. **Fracciones elementales.** La fracción racional propia $f/g \in P(X)$ se llama *elemental*, si $g = p^n$, $n \geqslant 1$, donde $p = p(X)$ es un polinomio irreducible, y, además, $\deg f < \deg p$.

El teorema fundamental sobre las fracciones racionales, es el

TEOREMA 3 *Cada fracción racional propia puede ser descompuesta, y, además, de la única manera, en una suma de fracciones elementales.*

DEMOSTRACION Esta se divide en dos partes: la existencia de la descomposición, y su unicidad.

1. Sea $f/g \in P(X)$ la fracción racional propia dada, en la que, sin limitación de generalidad, el polinomio g se puede considerar unitario. Supongamos que $g = g_1g_2$ es el producto de dos polinomios unitarios primos entre sí. De acuerdo con los resultados del § 3 tiene lugar la relación

$$1 = u_1g_1 + u_2g_2$$

con algunos $u_1, u_2 \in P[X]$. Multiplicando ambos miembros po f, obtendremos

$$f = fu_1g_1 + fu_2g_2.$$

Si $fu_1 = qg_2 + v_2$, $\deg v_2 < \deg g_2$, entonces,

$$f = v_1g_2 + v_2g_1, \tag{3}$$

donde $v_1 = qg_1 + fu_2$. Como $\deg v_2 < \deg g_2$, y $\deg f < \deg g$, en virtud de la condición de fracción propia, entonces, (3) puede cumplirse solamente cuando $\deg v_1 < \deg g_1$.

Dividiendo ambos miembros de la relación (3) por g_1g_2, obtendremos la descomposición de la fracción f/g en la suma de dos fracciones

$$f/g = v_1/g_1 + v_2/g_2,$$

además, ambas fracciones en el segundo miembro, son propias. Si en cualquiera de estas fracciones el denominador g_i es nuevamente el producto de dos polinomios primos entre sí, entonces, con respecto a esta fracción se pueden aplicar los razonamientos precedentes y obtener para ella una descomposición del mismo tipo. Operando de

este modo, llegamos en resumidas cuentas a la suma

$$\frac{f}{g}=\sum_{i=1}^{m}\frac{a_i}{p_i^{n_i}}, \tag{4}$$

m.c.d. $(a_i, p_i) = 1$, $\deg a_i < n_i \deg p_i$, donde los denominadores son las potencias $p_i^{n_i}$ de los polinomios unitarios irreducibles p_i, pertenecientes a la descomposición g:

$$g = p_1^{n_1}p_2^{n_2}\ \dots\ p_m^{n_m} \tag{5}$$

($p_i \neq p_j$ para $i \neq j$).

Expongamos la fracción propia a/p^n a una desintegración posterior. Como, por condición, $\deg a < n \deg p$, entonces, el algoritmo de división con resto nos lleva al sistema de igualdades

$$\begin{aligned} a &= q_1p^{n-1} + r_1, \\ r_1 &= q_2p^{n-2} + r_2, \\ &\dots\dots\dots\dots \\ r_{n-2} &= q_{n-1}p + r_{n-1}, \\ r_{n-1} &= q_n, \end{aligned}$$

donde $\deg q_i < \deg p$ para todos los cocientes $q_1, \dots, q_n$. Observamos, que

$$a = q_1p^{n-1} + q_2p^{n-2} + \dots + q_{n-1}p + q_n,$$

de donde

$$\frac{a}{p^n}=\frac{q_1}{p}+\frac{q_2}{p^2}+\dots+\frac{q_{n-1}}{p^{n-1}}+\frac{q_n}{p^n}.$$

Como $\deg q_i < \deg p$, entonces, las fracciones q_i/p^i son elementales.

II. Pasando a la cuestión de la unicidad de la descomposición, supongamos, que, excepto la representación obtenida por nosotros,

$$\frac{f}{g}=\sum_{i=1}^{m}\left(\sum_{j=1}^{n_i}\frac{a_{ij}}{p_i^j}\right), \quad \deg a_{ij} < \deg p_i \tag{6}$$

de la fracción propia f/g, en forma de la suma de fracciones elementales, se tiene otra descomposición más

$$\frac{f}{g}=\sum_{h=1}^{\mu}\left(\sum_{l=1}^{\nu_i}\frac{b_{hl}}{q_h^l}\right),$$

en la cual, posiblemente, se encuentran los sumandos b_{kl}/q_k^l con divisores q_k^l, que no figuran en (6). Agregando, si es necesario, en ambas expresiones de f/g sumandos con numeradores a_{ij} y b_{kl} nulos, y restando luego una expresión de la otra y reduciendo los términos

semejantes (con denominadores iguales), llegaremos a la identidad

$$\sum_{i=1}^{M}\left(\sum_{j=1}^{N_i}\frac{a_{ij}-b_{ij}}{p_i^j}\right)=0. \tag{7}$$

Aquí $M \leqslant m+\mu$ y para $i>m$, como p_i se toman algunos q_k, y N_i están elegidos de tal modo, que

$$a_{i,N_i}-b_{i,N_i}\neq 0. \tag{8}$$

Multiplicando la identidad (7) por $\prod_{i=1}^{M} p_i^{N_i}$, obtendremos la identidad polinomial

$$(a_{1,N_1}-b_{1,N_1})\prod_{i=2}^{M} p_i^{N_i}+p_1u=0.$$

La forma del polinomio u no nos interesa. Es importante, que de esta identidad se deduce la divisibilidad de $(a_{1,N_1}-b_{1,N_1})\prod_{i=2}^{M} p_i^{N_i}$ por p_1. Pero, el m.c.d. $\left(\prod_{i=2}^{M} p_i^{N_i} p_1\right)=1$, por eso, $p_1|(a_{1,N_1}-b_{1,N_1})$. Queda por recordar, que $\deg (a_{1,N_1}-b_{1,N_1})\leqslant \max\{\deg a_{1,N_1}, \deg b_{1,N_1}\}<\deg p_1$. Por lo tanto $a_{1,N_1}-b_{1,N_1}=0$, pese a la suposición (8). ∎

La demostración del teorema 3 es completamente constructiva (si se considera conocida la descomposición (4)) y puede ser usada para una representación efectiva de una fracción propia en forma de suma de fracciones elementales.

Notemos, que si $g=(X-c)^n h$, $h(c)\neq 0$, entonces,

$$\frac{f}{g}=\frac{b_1}{(X-c)^n}+\frac{f-b_1h}{(X-c)^n h}.$$

Haciendo $b_1=f(c)/h(c)$, obtendremos, $f(c)-b_1h(c)=0$ y, por lo tanto, $f-b_1h=(X-c)f_1$ (véanse el § 1 y el cap. 6). De este modo,

$$\frac{f-b_1h}{(X-c)^n h}=\frac{f_1}{(X-c)^{n-1} h}.$$

Aplicando el mismo procedimiento a esta fracción, menguamos en una unidad más el exponente de $X-c$ en el denominador, y así sucesivamente. Luego de n pasos llegamos a la descomposición

$$\frac{f}{g}=\frac{f}{(X-c)^n h}=\frac{f_0}{h}+\sum_{i=1}^{n}\frac{b_{1+n-i}}{(X-c)^i},\quad b_k\in P.$$

Si h (y, en consecuencia, $g = (X - c)^n h$) se descompone totalmente en factores lineales, entonces, separando por turno las fracciones elementales $b_{ki}(X - c_i)^k$ y utilizando, además, la propiedad de unicidad, por un camino un tanto distinto, llegaremos al resultado formulado en el teorema.

En el caso, cuando todos los factores irreducibles p_i en (4) son lineales o cuadráticos y, en consecuencia, las fracciones elementales tienen la forma

$$\frac{d}{(X-c)^n} \quad \text{o bien} \quad \frac{dX+e}{(X^2+aX+b)^n}; \qquad (9)$$
$$a, b, c, d, e \in P,$$

es también cómodo usar *el método de coeficientes indeterminados*. Este método consiste en que hay que escribir a f/g en forma de la suma de fracciones del tipo (9), multiplicando ambos miembros de la igualdad por g y, en la relación entre polinomios obtenida atribuir a X los valores convenientes de P para la obtención de los coeficientes $d, e, \ldots$ Como se deducirá de los resultados del capítulo siguiente, el método de los coeficientes indeterminados opera sin limitaciones, si P es un campo de números complejos o reales. Precisamente, sobre estos campos las fracciones elementales con mayor frecuencia se consideran como representando el papel de instrumento técnico en la integración de las funciones racionales.

EJERCICIOS

1. Construir el campo de relaciones $\mathbb{R}((X))$ del anillo $\mathbb{R}[[X]]$ de las series exponenciales formales de X con coeficientes en el campo $\mathbb{R}$. Apoyándose en el ejercicio 6 del § 3, mostrar que cada elemento del campo $\mathbb{R}((X))$ tiene la forma de la llamada *serie exponencial meromorfa*

$$\varphi(X) = a_{-m}X^{-m} + a_{-m+1}X^{-m+1} + \ldots + a_{-1}X^{-1} + a_0 + a_1X + a_2X^2 + \ldots, \quad a_i \in \mathbb{R},$$

en la cual se admite un número finito de exponentes negativos. En otras palabras, $\varphi(X) = X^{-m}f(X)$, donde $f(X)$ es una serie exponencial corriente de $\mathbb{R}[[X]]$.

2. Entenderemos por $\mathbb{R}(X, Y)$ (correspondientemente, $\mathbb{R}((X, Y))$) el campo de relaciones del anillo de los polinomios $\mathbb{R}[X, Y]$ (correspondientemente, del anillo íntegro $\mathbb{R}[[X, Y]]$; véase el ejercicio 7 del § 2). Muestra, que

$$\mathbb{R}(X, Y) = \{\mathbb{R}(X)\}(Y) = \{\mathbb{R}[X]\}(Y).$$

¿Son isomorfos los campos $\mathbb{R}((X, Y))$ y $\{\mathbb{R}((X))\}((Y))$? (*Respuesta*. No).

3. Sea la sucesión infinita de números reales $a_0, a_1, a_2, \ldots$ periódica, a partir de cierto término. Mostrar que la serie exponencial $f(X) = a_0 + a_1X + a_2X^2 + \ldots$ se escribe en forma de fracción racional de $\mathbb{R}(X)$.

4. Sean: K, un campo conmutativo con la unidad 1, no necesariamente íntegro; M, un submonoide del monoide multiplicativo en K, $S = K \times M$. Mostrar que la relación binaria $\Gamma \subset S^2$, definida por la relación

$$\Gamma = \{((a, b), (c, d)) \in S^2 \mid (ad - bc)u = 0, u \in M\}$$

(se tiene en cuenta cierto $u \in M$), es una relación de equivalencia en S. (*Indicación*. La reflexividad y la simetría de Γ son evidentes. Si ahora $((a, b), (c, d)) \in \Gamma$ y $((c, d), (e, f)) \in \Gamma$, de modo que $(ad - bc)\,u = 0$ y $(cf - de)\,v = 0$, para ciertos $u, v \in M$, entonces la primera igualdad debe multiplicarse por fv, y la segunda por bu. La suma miembro a miembro de las mismas determina la igualdad $(af - be)\,duv = 0$, con $duv \in M$, por cuanto $d, u, v \in M$, y M es un monoide. Por lo tanto $((a, b), (e, f)) \in \Gamma$, y la transitividad de Γ ha sido establecida).

5. Copiando la demostración del teorema 1, mostrar que en el factor conjunto S/Γ del conjunto $S = K \times M$, según la relación de equivalencia de Γ del ejercicio 4, se puede introducir la estructura del anillo conmutativo con unidad. Este anillo $Q_M(K)$ se llama anillo de los parciales sobre K con respecto a M. Para la integridad del anillo K y para $M = K^*$ se obtiene el habitual campo de parciales $Q(K)$. (*Indicación*. Sea $a/b = [a, b]$ una clase de equivalencia con representante $(b, a) \in S$. Introducir las dos operaciones binarias $\oplus \odot$:

$$a/b \oplus c/d = (ad + bc)/bd, \quad a/b \odot c/d = ac/bd,$$

y mostrar, que esta determinación no depende de la elección de los representantes. Puesto que $a/1 = c/1 \Leftrightarrow (a - c)\,u = 0$ para cierto $u \in M$, entonces el homomorfismo de los anillos $a \to a/1$ es un monomorfismo (inclusión) sólo para el anillo de integridad K y su submonoide M, que no contiene el cero).

6. Emplear la construcción $Q_M(K)$ al anillo $K = \mathbb{Z}$ con el monoide $M = \mathbb{Z} \,/\, p\mathbb{Z}$, compuesto por todos los números enteros, que no son divisibles por el número primo dado p. Mostrar que $Q_M(\mathbb{Z})$ se identifica con el conjunto de todos los números racionales a/b, con los b que no son divisibles por p.

Capítulo 6

RAÍCES DE LOS POLINOMIOS

Ocupémonos de aquello, para lo cual en el pasado se estudiaba álgebra: de las raíces de los polinomios. Esta cuestión ha dejado de ser dominante en el álgebra, pero su importancia no es discutida por nadie. El hecho es que muchos problemas de las matemáticas, en resumidas cuentas se reducen al cálculo de raíces aisladas de polinomios concretos, o a la descripción cualitativa del conjunto de ellas. Nos será posible tratar solamente las propiedades elementales de las raíces, pero ellas, en todo caso, serán suficientes para apreciar en plena medida el lugar especial que ocupa el campo $\mathbb{C}$ de los números complejos.

§ 1. PROPIEDADES GENERALES DE LAS RAÍCES

1. Raíces y factores lineales. Sea que el anillo conmutativo A con unidad está contenido en el anillo íntegro K.

DEFINICION. *El elemento $c \in K$ se llama raíz (o cero) del polinomio $f \in A[X]$, si $f(c) = 0$.* También se dice, que c es raíz de la ecuación $f(x) = 0$.

La necesidad de la consideración de los anillos, contenedores de A en forma propia, resulta comprensible, si se recuerda que el polinomio $f(X) = X^2 + 1$ sobre $\mathbb{R}$ no tiene ceros en $\mathbb{R}$, pero $f(i) = 0$, $i \in \mathbb{C} = \mathbb{R}[i]$. Primeramente consideremos, sin embargo, el caso en que $K = A$.

TEOREMA 1. (teorema de Bezout). *El elemento $c \in A$ es raíz del polinomio $f \in A[X]$ si, y sólo si, $X - c$ divide a f en el anillo $A[X]$.*

DEMOSTRACION. Este teorema es parte de una afirmación más general, que hubiésemos podido demostrar hace mucho. Y, precisamente, el algoritmo de división con resto (teorema 5 del § 2 del cap. 5) dice, que $f(X) = (X - c)\, q(X) + r(X)$, donde $\deg r(X) < \deg (X - c) = 1$. En consecuencia, $r(X)$ es una constante. La sustitución de c en lugar de X (o sea, el uso de la aplicación Π_c del teorema 2 del § 2 del cap. 5) da $f(c) = r$, así que siempre

$$f(X) = (X - c)\, q(X) + f(c). \tag{1}$$

En particular, $f(c) = 0 \Leftrightarrow f(X) = (X - c)\, q(X)$. ∎

La división del polinomio $f(X)$ con coeficientes en el anillo íntegro A, por el polinomio lineal $X - c$, es cómodo realizarla por el llamado *esquema de Horner*, más sencillo que el habitual algoritmo de división con resto. Precisamente, sea

$$f(X) = a_0 X^n + a_1 X^{n-1} + \ldots + a_n, \; a_i \in A.$$

De acuerdo con la fórmula (1)

$$q(X) = b_0X^{n-1} + b_1X^{n-2} + \ldots + b_{n-1}, \quad b_j \in A.$$

Igualando en esta fórmula los coeficientes para iguales potencias de X (comenzando por las mayores), luego de una pequeña transformación obtendremos

$b_0 = a_0$	$\ldots$	$b_k = b_{k-1}c + a_k$	$\ldots$	$b_{n-1} = b_{n-2}c + a_{n-1}$	$f(c) = b_{n-1}c + a_n$	. (2)

así que de paso se calcula el valor de f para $X = c$. Las fórmulas de recurrencia (2), en las que se encierra el «esquema de Horner», son cómodas para el cálculo.

En virtud del teorema 1, es natural introducir la siguiente, más general.

DEFINICIÓN. El elemento $c \in A$ se llama *raíz múltiple de k* (o *cero múltiple de k*) del polinomio $f \in A[X]$, si f se divide por $(X - c)^k$, pero no se divide por $(X - c)^{k+1}$. La raíz de multiplicidad 1 se llama *raíz simple* (correspondientemente, para $k = 2$ y 3 se habla de *raíz doble* y *triple*).

Así pues, $c \in A$ es una raíz de multiplicidad k del polinomio $f \in A[X]$ si, y sólo si, $f(X) = (X - c)^k g(X)$, donde m.c.d. $(X - c, g(X)) = 1$. La última condición, en virtud de la fórmula 1, se expresa también con la desigualdad $g(c) \neq 0$. Luego, en vista del teorema 1 del § 2 del cap. 5 observamos que $\deg f = k + \deg g$, de donde $k \leqslant \deg f$. Tiene lugar el importante

TEOREMA 2. *Sean A, un anillo íntegro; $f \neq 0$, un polinomio de $A[X]$ y $c_1, \ldots, c_r$, sus raíces en A con las respectivas multiplicidades $k_1, \ldots, k_r$. Entonces,*

$$f(X) = (X - c_1)^{k_1} \ldots (X - c_r)^{k_r} g(X),$$
$$g(X) \in A[X],\ g(c_i) \neq 0,\ i = 1, \ldots, r.$$

En particular, el número de raíces del polinomio $f \in A[X]$, consideradas junto con sus multiplicidades, no supera el grado del polinomio

$$k_1 + k_2 + \ldots + k_r \leqslant \deg f. \qquad (3)$$

DEMOSTRACIÓN. Es suficiente pasar al campo de relaciones $Q(A)$ (si es que el anillo A no era un campo desde el principio) y aprovecharse de la univocidad de la descomposición en factores primos (en este caso, en $X - c_1, \ldots, X - c_r$) en el anillo $Q(A)[X]$ (resultados de los §§ 3 y 4 del cap. 5). Sin embargo, no hay ahora necesidad de un arma tan potente. Razonaremos directamente.

Como $\deg f = (k_1 + \ldots + k_r) + \deg g$, entonces, la desigualdad (3) es consecuencia de la divisibilidad de f por $(X - c_1)^{k_1} \ldots$ $\ldots (X - c_r)^{k_r}$, que establecemos por inducción en r. Para $r = 1$

no hay nada que demostrar. Sea que ya sabemos que,

$$f(X) = (X - c_1)^{k_1} \ldots (X - c_{r-1})^{k_{r-1}} h(X).$$

Como tenemos que $c_r - c_1 \neq 0, \ldots, c_r - c_{r-1} \neq 0$ y A es un anillo íntegro, entonces, el elemento c_r no es raíz del polinomio $(X - c_1)^{k_1} \ldots (X - c_{r-1})^{k_{r-1}}$. Pero, c es la raíz de multiplicidad k_r del polinomio f, o sea, $f(X) = (X - c_r)^k u(X)$. Por eso, $h(c_r) = 0$. Correspondientemente, $h(X) = (X - c_r)^s v(X)$, $s \leqslant k_r$. Tenemos,

$$(X - c_r)^{k_r} u(X) = f(X) = (X - c_1)^{k_1} \ldots (X - c_{r-1})^{k_{r-1}} \times \times (X - c_r)^s v(X).$$

Utilizando la ley de simplificación en el anillo íntegro $A[X]$, llegamos a la conclusión de que $s = k_r$. ∎

Sin la hipótesis de la integridad del anillo A, el teorema 2 deja de ser cierto, como lo muestra el ejemplo del polinomio $f(X) = X^3$ sobre el anillo Z_8: $f(0) = f(2) = f(4) = f(6) = 0$. La descomposición de f en factores primos en $Z_8[X]$ tampoco es unívoca:

$$f = X^3 = X(X - 4)^2 = (X - 2)(X^2 + 2X + 4) = = (X - 6)(X^2 - 2X + 4).$$

Del teorema 2 se deduce el

COROLARIO. *Dos polinomios $f, g \in A[X]$ de grados $\leqslant n$, que adoptan iguales valores al sustituir $n + 1$ elementos distintos del anillo íntegro A, son iguales: $f = g$.*

DEMOSTRACIÓN. Hagamos $h = f - g$, así que $\deg h \leqslant n$. Por condición $h(c_1) = \ldots = h(c_{n+1}) = 0$ para distintos pares de elementos $c_1, \ldots, c_{n+1} \in A$, o sea, el polinomio h de grado $\leqslant n$, tiene por lo menos $n + 1$ raíces. La contradicción obtenida con respecto a la desigualdad (3) se puede eliminar, solamente reconociendo que $h = 0$. ∎

2. Funciones polinómicas. El corolario del teorema 2 permite resolver la cuestión antes tocada (véase el p. 1 del § 2 del cap. 5) sobre la relación entre los puntos de vista teorético-funcional y algebraico acerca de los polinomios. A cada polinomio $f \in A[X]$ se le pone en correspondencia la función

$$\tilde{f}: a \mapsto f(a), \quad \forall a \in A.$$

El conjunto de todas estas funciones constituye el anillo A_{pol} de las *funciones polinómicas* (o *racionales enteras*), que son un subanillo en el anillo de las funciones $A^A = \{A \to A\}$ con suma y multiplicación corrientes (véanse el ejemplo 3 en el p. 1 del § 4 del cap. 4, y el teorema 2, § 2, cap. 5). De un modo totalmente análogo, se introducen las funciones polinómicas de varias variables independientes.

Como ya se observó antes, el polinomio distinto de cero $X^2 + X \in \mathfrak{F}_2[X]$ define una función nula. En general, si $f(X) = (X^p - X)\, g(X)$ es un polinomio sobre un campo finito de p elementos, entonces, $\tilde{f}$ es una función nula, por cuanto $x^p - x = x(x^{p-1} - 1) = 0$, para todos los $x \in \mathfrak{F}_p$. Sólo en el caso en que $\deg f \leqslant \leqslant p-1$, el polinomio $f \in \mathfrak{F}_p[X]$ se determina por su función $\tilde{f}$. El polinomio arbitrario $f \in \mathfrak{F}_p[X]$ puede ser unívocamente sustituido por un determinado *polinomio reducido* f^* de grado $\leqslant p - 1$, tomando en calidad de f^* el resto de la división de f por $X^p - X$. Entonces, evidentemente, $\tilde{f} = \tilde{f}^*$.

En el caso de campos infinitos o de anillos íntegros, la situación es considerablemente más sencilla.

TEOREMA 4: *Si A es un anillo íntegro con un número infinito de elementos, entonces, la aplicación del anillo de los polinomios $A[X]$ en el anillo de las funciones polinómicas A_{pol}, definida por la correspondencia $f \to \tilde{f}$, es un isomorfismo.*

Hablando con propiedad, esto es una reformulación de corolario del teorema 2, por cuanto se habla solamente de confrontar al polinomio $f \neq 0$ con la función no nula $\tilde{f}$, o sea, $f(a) \neq 0$, aunque más no sea, para un $a \in A$. En realidad f no tiene más de n ceros en A, si $\deg f = n$. ∎

En base al teorema 3, el anillo de polinomios sobre el campo infinito P se identifica con el anillo de las funciones polinómicas (designadas $f(x)$ con la letra latina minúscula x), y queda sólo por resolver la cuestión de cómo por $\tilde{f}$ (y de hecho, por algunos valores del polinomio f) reconstruir en forma explícita el propio polinomio.

La exacta formulación del problema de la «interpolación» se reduce a lo siguiente. Sean $b_0, b_1, \ldots, b_n$, (respectivamente, $c_0, c_1, \ldots, c_n$), $n + 1$ elementos cualesquiera (respectivamente, *distintos*) del campo P. Se requiere hallar el polinomio $f \in P[X]$ de grado $\leqslant n$, tal que $f(c_i) = b_i$, $i = 0, 1, \ldots, n$. De acuerdo con el corolario del teorema 2 la solución del problema, si es que existe, es única. Pero un polinomio f con las propiedades dadas siempre existe, como lo muestra la *fórmula de interpolación de Lagrange*

$$f(X) = \sum_{i=0}^{n} b_i \frac{(X - c_0) \ldots (X - c_{i-1})(X - c_{i+1}) \ldots (X - c_n)}{(c_i - c_0) \ldots (c_i - c_{i-1})(c_i - c_{i+1}) \ldots (c_i - c_n)}. \qquad (4)$$

Por otra parte, la existencia y la unicidad de la solución se percibe inmediatamente del sistema lineal

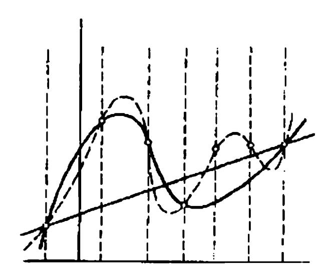
$$\begin{aligned} a_0 c_0^n + a_1 c_0^{n-1} + \ldots + a_n &= b_0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_0 c_n^n + a_1 c_n^{n-1} + \ldots + a_n &= b_n \end{aligned}$$

para los coeficientes $a_0, \ldots, a_n$ del polinomio buscado f. El determinante de este sistema, que es un determinante de Vandermonde, es distinto de cero, y las a_i se encuentran por la regla de Crámer. La

comodidad de la fórmula (4) se debe a su sencillez y a la facilidad con que se la retiene en la memoria. Algunas ventajas tiene a veces la *fórmula de interpolación de Newton*

$$f(X) = u_0 + u_1(X - c_0) + \ldots + u_n(X - c_0)(X - c_1) \ldots \\ \ldots (X - c_{n-1}), \quad (5)$$

donde los coeficientes $u_0, u_1, \ldots, u_n$ se determinan por medio de la sustitución sucesiva de los valores $X = c_0, X = c_1, \ldots, X = c_n$. Las fórmulas de interpolación (4), (5), hallan utilización práctica en



el cálculo y en la representación gráfica de la función $\varphi: \mathbb{R} \to \mathbb{R}$, dada por una tabla u obtenida en la práctica. Sabiendo, por algunos razonamientos indirectos, que la función φ se comporta lo suficientemente bien en el intervalo I de la recta real $\mathbb{R}$, se trata de representar a φ en I por una función tan «lisa» como la polinómica. Además, en calidad de los llamados «nudos de interpolación» se utiliza una parte de los puntos $c_0, c_1, \ldots, c_n$ dentro del intervalo I, en los cuales (y sólo en ellos) se conocen los valores de $\varphi(c_i) = b_i$. A la delicada cuestión de la elección de los nudos de interpolación y a la elaboración de los métodos generales de aproximación de las funciones, se les han dedicado secciones enteras de las matemáticas. Cabe anotar, que el uso de los procesos de interpolación jugó un gran papel en el desarrollo de la teoría de los números trascendentes (la definición de los números algebraicos y trascendentes, véase en el § 2 del cap. 5), así que aquí convergen los intereses de la teoría de funciones, de la teoría de los números y del áblegbra.

Observemos finalmente, que a cada fracción racional irreducible $f/g \in P(X)$ (véase el § 4 del cap. 5) y a cada ampliación $F \supset P$ con un número infinito de elementos, se les confronta la *función racional* $\widetilde{f/g}$: $F_{(f/g)} \to F$ con campo de definición $F_{(f/g)}$, obtenida de F por separación de un número finito de elementos nulos del polinomio g en F. Se puede demostrar, que para las condiciones dadas, la aplicación $f/g \to \widetilde{f/g}$ es biunívoca. Esta afirmación no nos es nece-

saria. Intuitivamente ella es clara. A pesar de esta correspondencia, hay que hacer una diferenciación precisa entre las fracciones racionales y las funciones racionales. La función racional $x \mapsto 1/x$ no está definida en el punto $x = 0$, al mismo tiempo que la cuestión de la determinación de la fracción racional $1/X$ en general no se plantea.

3. Diferenciaciones del anillo de polinomios. El punto de vista funcional sobre los polinomios, hace natural la siguiente definición. Sea

$$f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$$

un polinomio de grado n sobre el campo P. Se llama derivada del mismo al polinomio

$$f'(X) = na_0X^{n-1} + (n-1)a_1X^{n-2} + \ldots + a_{n-1}. \tag{6}$$

Si $P = \mathbb{R}$ es el campo de números reales, y $\tilde{f}$ es una función polinómica vinculada con f, entonces, la definición (6) de derivada coincide con la habitual definición de la misma como límite

$$\lim_{\Delta x \to 0} \frac{\tilde{f}(x+\Delta x) - \tilde{f}(x)}{\Delta x}.$$

En el caso de un campo P arbitrario, hablar de cualquier propiedad de continuidad de la función polinómica no tiene sentido (¿qué es una sucesión convergente en Z_p?) y es necesario partir de la definición formal de (6).

Tienen lugar las relaciones, bien conocidas en el análisis matemático

$$(\alpha f + \beta g)' = \alpha f' + \beta g', \quad \alpha, \beta \in P, \tag{7}$$

$$(fg)' = f'g + fg'. \tag{8}$$

La relación (7) se deduce directamente de (6) y de la definición de suma de polinomios. Utilizando (7) y la definición de producto de polinomios, la comprobación de (8) se puede llevar al caso cuando $f = X^k$, $g = X^l$:

$$(X^{k+l})' = (k+l)X^{k+l-1} = (kX^{k-1})X^l + X^k(lX^{l-1}) =$$
$$= (X^k)'X^l + X^k(X^l)'.$$

Sirve de generalización de (8) la fórmula fácilmente demostrable por inducción en k,

$$(f_1f_2 \ldots f_k)' = \sum_{i=1}^{k} f_1 \ldots f_{i-1}f_i'f_{i+1} \ldots f_k.$$

En particular,

$$(f^k)' = kf^{k-1}f'. \tag{9}$$

Las relaciones (7), (8), reescritas en términos de la aplicación $\frac{d}{dX}: f \mapsto f'$ (también se dice que $\frac{d}{dX}$ es un *operador de diferenciación*)

sugieren la idea de introducir para su examen la aplicación $\mathscr{D}: K \to K$, para el anillo arbitrario K, poseedora de las propiedades

$$\mathscr{D}(u+v)=\mathscr{D}u+\mathscr{D}v, \tag{7'}$$

$$\mathscr{D}(uv)=(\mathscr{D}u)v+u(\mathscr{D}v). \tag{8'}$$

Tal género de aplicaciones del anillo K en sí mismo, llamadas *diferenciaciones*, son muy útiles para el estudio de K, y el conjunto de ellas Der (K) resulta un objeto muy interesante, que sirve de introducción en un amplio dominio de las matemáticas (*grupos y álgebras de Lie*).

Sirve de generalización de (8′) la fórmula de Leibniz

$$\mathscr{D}^m(uv)=\sum_{k=0}^{m}\binom{m}{k}\mathscr{D}^k u\mathscr{D}^{m-k}v, \tag{8''}$$

obtenida por inducción en $m \geqslant 1$ (aplicación de $\mathscr{D}$ a (8″), el uso de (8′) y la relación $\binom{m}{k-1}+\binom{m}{k}=\binom{m+1}{k}$ dan (8″) para $m+1$).

En el caso de $K=P[X]$, de las relaciones (7′), (8′), complementadas por la regla

$$\mathscr{D}(\lambda f)=\lambda\mathscr{D}f, \quad \lambda \in P,$$

se deduce inmediatamente, que

$$\mathscr{D}f(X)=f'(X)\,\mathscr{D}X.$$

De este modo, cualquier diferenciación del anillo de los polinomios $P[X]$ se determina dando un único polinomio $\mathscr{D}X$. Para $\mathscr{D}X=1$ obtenemos el habitual operador de diferenciación $\frac{d}{dX}$.

4. Factores múltiples. El resultado de utilizar m veces consecutivas la aplicación $\frac{d}{dX}$ a $f(X)$ habitualmente se designa con el símbolo $f^{(m)}(X)$. Es evidente, que

$$f(X)=a_0X^n+a_1X^{n-1}+\ldots+a_n \Rightarrow$$
$$\Rightarrow f^{(n)}(X)=n!a_0, \quad f^{(n+1)}(X)=0.$$

Si P es un campo de característica nula, entonces,

$$\deg f'=\deg f-1.$$

Sin embargo, para los campos de característica finita p esto ya no es así, por cuanto

$$(X^{kp})'=kpX^{kp-1}=0.$$

De cualquier modo, alguna utilidad de la consideración de la derivada se puede obtener también en el caso general. Dividiendo el polinomio arbitrario $f \in P[X]$ por $(X-c)^2$, $c \in F$, $F \supset P$, y escribiendo luego el resto (lineal) en forma de $(X-c)s+r$, donde $s, r \in F$, llegamos a las relaciones $f=(X-c)^2t+(X-c)s+r$,

$f' = (X - c)[2t + (X - c)t'] + s$. Sustituyendo en ellas el valor $X = c$, obtenemos $r = f(c)$, $s = f'(c)$, o sea,

$$f(X) = (X - c)^2 t(X) + (X - c) f'(c) + f(c).$$

Arribamos a la siguiente afirmación.

TEOREMA 4 *Sean P, un campo arbitrario, y F' una ampliación cualquiera de este campo. El polinomio $f \in P[X]$ tiene raíz múltiple $c \in F$ si, y solo si, $f(c) = f'(c) = 0$.* ∎

EJEMPLO 1. En cualquier campo de característica p, el polinomio $X^n - 1$ tiene solamente raíces simples, si n no se divide por p. Efectivamente, las raíces de la derivada nX^{n-1} no pueden ser raíces de $X^n - 1$.

A continuación se supone que P es un campo de característica nula y que sin limitación de generalidad se puede entender por P uno de los campos $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. El polinomio irreducible unitario $p_i(X)$ en la descomposición

$$f(X) = \lambda p_1(X)^{k_1} \ldots p_i(X)^{k_i} \ldots p_r(X)^{k_r}, \quad \lambda \in P \qquad (10)$$

del polinomio $f(X) \in P[X]$ se llama (por analogía con la definición de raíz múltiple) factor de multiplicidad k_i para f. Anteriormente, ya se dijo que obtener la descomposición (10) en la práctica es bastante difícil. Describamos brevemente el método basado en el concepto de derivada y que da la posibilidad de saber, si $f(X)$ contiene factores múltiples sobre el campo P dado (o sobre su ampliación).

TEOREMA 5 *Sea $p(X)$ un factor irreducible de multiplicidad k del polinomio $f \in P[X]$ ($k \geqslant 1$, $\deg p(X) \geqslant 1$). Entonces, $p(X)$ será un factor de multiplicidad $(k - 1)$ de la derivada $f'(X)$. En particular, para $k = 1$, f' no se divide por $p(X)$.*

DEMOSTRACIÓN Por condición $f(X) = p(X)^k g(X)$, donde el m.c.d. $(p(X), g(X)) = 1$, o sea, $g(X)$ no se divide por $p(X)$. Empleando las reglas (8) y (9), hallamos

$$f'(X) = p(X)^{k-1}[kp'(X) g(X) + p(X) g'(X)].$$

Es suficiente mostrar, que el polinomio encerrado entre corchetes no se divide por $p(X)$. Si esto no fuera así, entonces, el polinomio $kp'(X) g(X)$ se dividiría por $p(X)$, lo que sin embargo, es imposible (véanse los corolarios de los teoremas 3 y 4 del § 3 del cap. 5), por cuanto $g(X)$ no se divide por $p(X)$, y $\deg kp'(X) < \deg p(X)$. ∎

Es claro, que en el curso de la demostración se usaron, esencialmente, la irreducibilidad de $p(X)$ y la condición char $P = 0$.

COROLARIO 1 *Para el polinomio $f(X)$ con coeficientes en el campo P de característica cero, las dos condiciones siguientes son equivalentes:*

(i) *En alguna ampliación $F \supset P$ del campo P, f tiene una raíz con multiplicidad k;*

(ii) $f^{(j)}(c) = 0$, $1 \leqslant j \leqslant k - 1$, pero $f^{(k)}(c) \neq 0$.

Para demostrarlo, hay que usar k veces el teorema 5, teniendo en cuenta el factor lineal $p(X) = X - c$ y sustituyendo desde un principio, en caso de necesidad, P por su ampliación F, contenedora de la raíz c. ■

COROLARIO 2. *Si el polinomio $f \in P[X]$ de grado ≥ 1 tiene la descomposición* (10), *entonces, la descomposición del máximo común divisor de f y de su derivada f' será*

$$\text{m.c.d.}\,(f, f') = p_1(X)^{k_1-1} p_2(X)^{k_2-1} \ldots p_r(X)^{k_r-1} \qquad (11)$$

(el m.c.d. *siempre puede ser considerado como polinomio unitario*).

Efectivamente, por el teorema 5, cada uno de los divisores primos $p_i(X)$ del polinomio $f(X)$ con la descomposición canónica (10), entra en la descomposición de $f'(X)$ con el exponente $k_i - 1$, o sea,

$$f'(X) = p_1(X)^{k_1-1} p_2(X)^{k_2-1} \ldots p_r(X)^{k_r-1} u(X),$$

donde m.c.d. $(u, p_i) = 1$, $1 \leq i \leq r$ (se supone que $p_i(X)^0 = 1$). Por esto, de acuerdo con el conocido criterio de divisibilidad (véase el punto 2, § 3 del cap. 5), concluimos que el m.c.d. (f, f') se calcula por la fórmula (11). ■

Utilizando la expresión (11) para el m.c.d. (f, f'), obtenemos un medio para liberarnos de los factores múltiples que entran en la descomposición de $f(X)$. Precisamente, el polinomio

$$g(X) = \frac{f(X)}{\text{m.c.d.}\,(f, f')} = p_1(X)\, p_2(X) \ldots p_r(X)$$

contiene los mismos divisores primos que $f(X)$, pero con multiplicidad unitaria. Es importante señalar que el polinomio $g(X)$ se puede hallar desconociendo de hecho las descomposiciones para f y f', usando solamente el algoritmo de Euclides.

EJEMPLO 2. El polinomio $f(X) = X^5 - 3X^4 + 2X^3 + 2X^2 - 3X + 1$ y su derivada $f'(X) = 5X^4 - 12X^3 + 6X^2 + 4X - 3$ tienen en calidad de m.c.d. el polinomio unitario $X^3 - 3X^2 + 3X - 1 = (X - 1)^3$. El polinomio «libre de cuadrados» $g(X) = f(X)/(X - 1)^3 = X^2 - 1 = (X - 1)(X + 1)$ tiene dos raíces ± 1. De este modo, $f(X) = (X - 1)^4 (X + 1)$ posee la raíz 1 de multiplicidad 4 y la raíz simple -1.

5. Fórmulas de Viete. En relación con la teoría de los sistemas de ecuaciones lineales, ya tuvimos la oportunidad de hacer mención acerca de la influencia favorable que tuvo sobre su evolución el buen sistema de designaciones, que llevó, en particular, a los determinantes. Esto es mérito de los matemáticos del siglo XVIII y de principios del XIX. Pero, mucho antes, cuando el Algebra aún se confundía con el «análisis de ecuaciones», los perfeccionamientos decisivos de las desiganciones algebraicas de F. Viete y R. Descartes tocó la teoría de los polinomios y de las ecuaciones algebraicas. De los tipos particulares de ecuaciones con coeficientes numéricos,

que escondían las leyes generales, fue dado un paso audaz a las ecuaciones con coeficientes literales. La nueva forma de escritura frecuentemente genera nuevos resultados. Para Descartes esto concluyó en la revolucionaria aplicación del álgebra a la geometría. Nos detendremos en el logro más modesto de su antecesor Viete.

Supongamos, que el polinomio $f \in P[X]$ unitario (con coeficiente mayor $= 1$) de grado n, tiene en el campo P, o en alguna ampliación del mismo, n raíces $c_1, c_2, \ldots, c_n$, entre las cuales, posiblemente, las hay iguales. Entonces, en correspondencia con el teorema 2, es legítima la descomposición

$$f(X) = (X - c_1)(X - c_2)\ldots(X - c_n).$$

Escribamos $f(X)$ en forma habitual, por potencias de X:

$$f(X) = X^n + a_1X^{n-1} + \ldots + a_kX^{n-k} + \ldots + a_n,$$

para ello multipliquemos todos los binomios $X - c_i$ y simplifiquemos los términos semejantes. Entonces, para los coeficientes $a_1, \ldots, a_n$ se obtienen expresiones por medio de las raíces $c_1, \ldots, c_n$:

$$\begin{aligned} a_1 &= -(c_1 + c_2 + \ldots + c_n), \\ &\ldots\ldots\ldots\ldots \\ a_k &= (-1)^k \sum_{i_1 < i_2 < \ldots < i_k} c_{i_1}c_{i_2}\ldots c_{i_k}, \qquad (12) \\ &\ldots\ldots\ldots\ldots \\ a_n &= (-1)^n c_1c_2\ldots c_n. \end{aligned}$$

Las fórmulas (12) se llaman *fórmulas de Viete.*

Si el polinomio f no fuera unitario, o sea, si tuviera el coeficiente mayor $a_0 \neq 1$, entonces, las fórmulas análogas a (12), darían la expresión de la relación a_i/a_0.

Las fórmulas de Viete, que establecen una relación implícita entre las raíces y los coeficientes de un polinomio arbitrario (unitario), son notables por el hecho de que sus segundos miembros no varían para cualesquiera permutaciones de las raíces $c_1, \ldots, c_n$. Esto nos da lugar a introducir el concepto de *función simétrica*, del mismo modo que, en relación con los determinantes resultó cómodo examinar las funciones antisimétricas generales. De acuerdo con la definición dada en el corolario del teorema 3' del punto 2 del § 2 del cap. 5, el elemento π del grupo simétrico S_n opera en la función $\tilde{f}(x_1, \ldots, x_n)$ de n argumentos de acuerdo a la regla

$$(\pi\tilde{f})(x_1, \ldots, x_n) = \tilde{f}(x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)}).$$

La función $\tilde{f}$ se llama simétrica, si $\pi\tilde{f} = \tilde{f}$ para todos los $\pi \in S_n$. Sirven de ejemplos de funciones simétricas las llamadas *funciones*

simétricas elementales s_k:

$$s_k(x_1, \ldots, x_n) = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} x_{i_1} x_{i_2} \ldots x_{i_k}. \qquad (13)$$

Ellas permiten reescribir las fórmulas (12) en la forma

$$a_k = (-1)^k s_k(c_1, \ldots, c_n), \quad k = 1, 2, \ldots, n, \qquad (12')$$

así que con exactitud hasta el signo, el coeficiente a_k del polinomio f es valor de la función s_k en el conjunto de las raíces del polinomio f. Prestemos atención al hecho de que, por definición, $a_k \in P$, aunque las raíces $c_1, \ldots, c_n$, hablando en general, están en alguna ampliación $F \supset P$. La cuestión de la existencia de F no se toca por ahora. Pero, a veces, la descomposición de un polinomio en factores lineales es consecuencia directa de las propiedades del campo P.

EJEMPLO. Consideremos el polinomio $X^{p-1} - 1$ sobre el campo finito $\mathbb{F}_p$. Sabemos que $x^{p-1} = 1$ para todos los $x \in \mathbb{F}_p^*$, o sea, todos los elementos no nulos son raíces del polinomio $X^{p-1} - 1$. Por consiguiente, tiene lugar la descomposición

$$X^{p-1} - 1 = (X - 1)(X - 2) \ldots (X - (p - 1)). \qquad (14)$$

Se supone que nos hemos familiarizado con el campo $\mathbb{F}_p$ en tal grado que distinguimos sin dificultad la naturaleza dual de los números $1, 2, \ldots, p - 1$ como elementos ordinarios de $\mathbb{Z}$ y como elementos del campo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (representantes de las clases de restos $\{i\}_p$). De (7), (6) y (8) obtenemos

$$s_k(1, 2, \ldots, p - 1) \equiv 0 \pmod p, \quad k = 1, \quad 2, \quad \ldots, \quad p - 2,$$
$$s_{p-1}(1, 2, \ldots, p - 1) \equiv -1 \pmod p.$$

La última relación, escrita de nuevo en la forma

$$(p - 1)! + 1 \equiv 0 \pmod p \qquad (15)$$

y conocida como tal bajo el nombre de teorema de Vilson, expresa el realmente necesario y suficiente criterio de simplicidad de un número entero p. Efectivamente, acabamos de demostrar el cumplimiento de (15) para los p primos. Por otro lado, $p = p_1p_2 \Rightarrow (p - 1)! = p_1 t \Rightarrow (p - 1)! + 1 \not\equiv 0 \pmod{p_1} \Rightarrow$ $\Rightarrow (p - 1)! + 1 \not\equiv 0 \pmod p$. ■

EJERCICIOS

1. ¿Será íntegro el anillo de las funciones polinómicas sobre el campo de p elementos?

2. Sean P un campo infinito, y f, un polinomio no nulo de $P(X_1, \ldots, X_n)$. Basándose en el teorema 3 y utilizando la inducción en n, demostrar la existencia de $a_1, \ldots, a_n \in P$, para los cuales $f(a_1, \ldots, a_n) \neq 0$. Esto da el isomorfismo $P[X_1, \ldots, X_n]$ con un anillo de funciones polinómicas de n variables sobre P.

3. El polinomio no nulo $f \in Z_p[X_1, \ldots, X_n]$ de grado $< p$ en cada variable posee la propiedad formulada en el ejercicio 2: $f(a_1, \ldots, a_n) \neq 0$ para los cuales $a_1, \ldots, a_n \in Z_p$. Mostrar que cualquier polinomio $f \in Z_p[X_1, \ldots, X_n]$ puede ser escrito en la forma

$$f(X_1, \ldots, X_n) = \sum_{i=1}^{n} g_i(X_1, \ldots, X_n)(X_i^p - X_i) + f^*(X_1, \ldots, X_n),$$

(ii) Sea $f(X_1, \ldots, X_n)$ una forma (polinomio homogéneo) de grado m. Convencerse de la legitimidad de *la identidad de Euler*

$$\sum_{k=1}^{n} X_k \frac{\partial f}{\partial X_k} = m \cdot f(X_1, \ldots, X_n).$$

A la inversa, si char $P = 0$, entonces, la identidad de Euler se satisface solamente por las formas de grado $m = 1, 2, 3, \ldots$

10. Mostrar, que la ausencia de factores lineales en el polinomio $X^n + a_1X^{n-1} + \ldots + a_n \in Z_2[X]$ es equivalente al cumplimiento de la condición $a_n (1 + \sum a_i) \neq 0$. Para $n \leqslant 3$ los polinomios irreducibles sobre Z_2 se agotan con los siguientes: X, $X+1$, X^2+X+1, X^3+X+1, X^3+X^2+1. Acotar todos los polinomios irreducibles sobre Z_2 para $n = 4$ y 5 (ellos serán, respectivamente, 3 y 6).

11. A partir de la congruencia

$$X^5 - X^2 + 1 \equiv X^2(X+1)(X^3+X+1) \pmod 2$$

establecer la irreductibilidad del polinomio $X^5 - X^2 + 1$ sobre $\mathbb{Q}$. (*Indicación*. Utilizar el corolario del lema de Gauss (3. del cap. 5) y el ejercicio anterior, y también fundarse en la factorizabilidad del anillo $Z_2[X]$.)

Análogamente, demostrar la irreductibilidad del polinomio $X^5 - X - 1$ sobre $\mathbb{Q}$, pasando a la congruencia por mod 3.

§ 2. POLINOMIOS SIMÉTRICOS

1. Anillo de los polinomios simétricos. Siguiendo la definición de funciones simétricas, dada al final del parágrafo anterior, introducimos un concepto análogo en el anillo $A[X_1, \ldots, X_n]$ de los polinomios sobre el anillo íntegro A. El teorema 3 del § 1, extendido a los polinomios y funciones de muchas variables, parece hacer superfluo este traslado. Pero, hay que considerar, que en este teorema el anillo íntegro A de los coeficientes es infnito, mientras que nosotros queremos tener una estructura universal.

Y bien, recurriendo de nuevo al corolario del teorema 3' del punto 2, § 2 del cap. 6, ponemos en correspondencia con cada permutación $\pi \in S_n$ el automorfismo $\tilde{\pi}: A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_n]$, que traslada el polinomio arbitrario $f \in A[X_1, \ldots, X_n]$ en el polinomio πf:

$$(\pi f)(X_1, \ldots, X_n) = f(X_{\pi^{-1}(1)}, \ldots, X_{\pi^{-1}(n)}).$$

El polinomio f se llama *simétrico*, si $\pi f = f$ para todos $\pi \in S_n$. Al igual que para las funciones, se introducen los polinomios simétricos elementales s_k:

$$s_k(X_1, \ldots, X_n) = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} X_{i_1} X_{i_2} \ldots X_{i_k}.$$

Hablando en rigor, hubiese correspondido examinar el polinomio

$$f(Y) = (Y - X_1)(Y - X_2) \ldots (Y - X_n) = Y^n - s_1Y^{n-1} + s_2Y^{n-2} + \ldots + (-1)^n s_n \qquad (2)$$

sobre $A[X_1, \ldots, X_n]$ de la nueva variable Y, y observar, que s_k es un polinomio simétrico, por cuanto el primer miembro de la identidad (2) no varía para cualesquiera permutaciones de los factores lineales $Y - X_1, \ldots, Y - X_n$.

Prestemos atención a la circunstancia de que, luego de sustituir X_n por cero en ambos miembros de la identidad (2), obtendremos

$$(Y - X_1) \ldots (Y - X_{n-1}) Y = Y^n - (s_1)_0 Y^{n-1} + \ldots$$
$$\ldots + (-1)^{n-1} (s_{n-1})_0 Y,$$

donde $(s_k)_0$ es el resultado de la sustitución $X_n = 0$ en s_k. Simplificando ambos miembros por Y (en base al teorema 3, § 4 del cap. 5, aplicado a $A[X_1, \ldots, X_n, Y]$), llegamos a la identidad

$$(Y - X_1)(Y - X_2) \ldots (Y - X_{n-1}) =$$
$$= Y^{n-1} - (s_1)_0 Y^{n-2} + \ldots + (-1)^{n-1} (s_{n-1})_0. \quad (3)$$

Comparando (2) con (3), *llegamos a la conclusión, de* que $(s_1)_0, \ldots$ $\ldots (s_{n-1})_0$, *son polinomios simétricos elementales de las $n-1$ variables* $X_1, \ldots, X_{n-1}$.

Como, además, π es un automorfismo del anillo $A[X_1, \ldots, X_n]$, entonces, cualesquiera combinaciones lineales de polinomios simétricos y de sus productos, de nuevo serán polinomios simétricos. Esto significa, que el *conjunto de todos los polinomios simétricos forma un anillo, que es subanillo del anillo* $A[X_1, \ldots, X_n]$. Nuestra tarea inmediata, es comprender la conformación de este subanillo.

2. Teorema fundamental de los polinomios simétricos. Resulta, que el método más general de obtención de polinomios simétricos, es el siguiente. Hay que tomar un polinomio arbitrario $g \in A[Y_1, \ldots, Y_n]$ y sustituir $Y_1, \ldots, Y_n$ por $s_1, \ldots, s_n$, respectivamente. Como resultado, se obtiene el polinomio

$$f(X_1, \ldots, X_n) = g(s_1(X_1, \ldots, X_n), \ldots, s_n(X_1, \ldots, X_n))$$

que es, por supuesto, simétrico.

Observamos también, que el monomio $Y_1^{i_1}, \ldots, Y_n^{i_n}$, que forma parte de g, al sustituir $Y_k = s_k(X_1, \ldots, X_n)$ pasa a ser un polinomio homogéneo de $X_1, \ldots, X_n$ de grado $i_1 + 2i_2 + \ldots + ni_n$, por cuanto $\deg s_k = k$.

La suma $i_1 + 2i_2 + \ldots + ni_n$ se llama habitualmente *peso del monomio* $Y_1^{i_1} \ldots Y_n^{i_n}$. Es natural considerar como *peso del polinomio* $g(Y_1, \ldots, Y_n)$ al máximo de los pesos de los monomios que entran en g.

La afirmación fundamental acerca de los polinomios simétricos la expresa el

TEOREMA 1. *Sea $f \in A[X_1, \ldots, X_n]$, un polinomio simétrico de grado total m sobre el anillo íntegro A. Entonces, existe, y además es*

único, un polinomio $g \in A[Y_1, \ldots, Y_n]$ *de peso* m *para el cual*

$$f(X_1, \ldots, X_n) = g(s_1, \ldots, s_n).$$

La demostración se compondrá de dos partes.

I. DEMOSTRACION DE LA EXISTENCIA DEL POLINOMIO g. Utilizamos la inducción para dos parámetros n y m (véase el § 7 del cap. 1). Para $n = 1$, el teorema es evidente, por cuanto $s_1 = X_1$ y $f(X_1) = f_1(s_1)$. Suponiendo que la afirmación sobre la existencia de g ha sido demostrada para los polinomios de $\leqslant n - 1$ variables, razonaremos, en caso de n variables, por inducción para $m = \deg f$. Como para $m = 0$ no hay nada que demostrar, entonces, suponemos $m > 0$ y consideramos establecida la existencia de g para cualquier polinomio de grado $< m$.

Sea ahora $f(X_1, \ldots, X_n)$ el polinomio simétrico dado de grado m. Haciendo $X_n = 0$ tendremos, por presupuesto de la inducción

$$f(X_1, \ldots, X_{n-1}, 0) = g_1((s_1)_0, \ldots, (s_{n-1})_0),$$

donde g_1 es algún polinomio de $A[Y_1, \ldots, Y_{n-1}]$ de peso $\leqslant m$ (el grado de f, con la sustitución $X_n = 0$ puede mermar), y $(s_1)_0, \ldots, (s_{n-1})_0$ son polinomios simétricos elementales de $X_1, \ldots, X_{n-1}$ (véase (3)). Además, evidentemente, $\deg g_1(s_1, \ldots, s_{n-1}) \leqslant m$. De este modo, el polinomio

$$f_1(X_1, \ldots, X_n) = f(X_1, \ldots, X_n) - g_1(s_1, \ldots, s_{n-1}) \qquad (4)$$

tiene un grado total en $X_1, \ldots, X_n$ no mayor que m y (como diferencia de dos polinomios simétricos) es simétrico. Además, $f_1(X_1, \ldots, X_{n-1}, 0) = 0$, de donde se deduce, que X_n divide a $f_1 : f_1 = X_n \cdot f^\circ$. Pero en virtud de la simetría de $f_1 = \pi^{-1} f_1 = X_{\pi(n)}(\pi^{-1} f^\circ)$, $\forall \pi \in S_n$, o sea, f_1 contiene en calidad de factores a $X_1, X_2, \ldots, X_n$, y, en consecuencia, y el producto de los mismos $s_n = X_1 X_2 \ldots X_n$. Así pues,

$$f_1(X_1, \ldots, X_n) = s_n \cdot f_2(X_1, \ldots, X_n), \qquad (5)$$

donde f_2 es de nuevo un polinomio simétrico, esta vez de grado $\deg f_2 = \deg f_1 - n \leqslant m - n$. Por presupuesto de la inducción, existe un polinomio $g_2(Y_1, \ldots, Y_n)$ de peso $\leqslant m - n$, para el cual $f_2(X_1, \ldots, X_n) = g_2(s_1, \ldots, s_n)$. Teniendo en cuenta (4) y (5), para f obtenemos la expresión

$$f(X_1, \ldots, X_n) = g_1(s_1, \ldots, s_{n-1}) + s_n g_2(s_1, \ldots, s_n),$$

y la existencia del polinomio $g = g_1(Y_1, \ldots, Y_n) + Y_n g_2(Y_1, \ldots, Y_n)$ de peso $\leqslant m$, queda determinada. Como $\deg f = m$, entonces, el peso del polinomio g no puede ser menor que m y, por lo tanto, es exactamente igual a m.

II. DEMOSTRACION DE LA UNICIDAD. Si existieran dos polinomios g_1, g_2, distintos entre sí, con la condición $f = g_1(s_1, \ldots, s_n) = g_2(s_1, \ldots, s_n)$, entonces, tendríamos el polinomio $g(Y_1, \ldots$

$\ldots, Y_n) = g_1 - g_2 \neq 0$, para el que $g(s_1, \ldots, s_n) = 0$. En otras palabras, $s_1, \ldots, s_n$ resultarían algebraicamente dependientes sobre A, en el sentido de la definición del punto 2, § 2, del cap. 5. Mostremos (otra vez por inducción en n), que esto no es así. Efectivamente, razonando a la inversa, elijamos un polinomio $g(Y_1, \ldots$ $\ldots, Y_n)$ de grado mínimo, que se reduce a cero con la sustitución $Y_k = s_k$. Considerando a g como un polinomio en Y_n sobre $A[Y_1, \ldots, Y_{n-1}]$, lo escribimos en la forma

$$g(Y_1, \ldots, Y_n) = g_0(Y_1, \ldots, Y_{n-1}) + \ldots$$
$$\ldots + g_k(Y_1, \ldots, Y_{n-1}) Y_n^k, \quad k = \deg_n g.$$

Si $g_0 = 0$, entonces, $g = Y_n h$, donde $h \in A[Y_1, \ldots, Y_n]$. Por suposición $s_n h(s_1, \ldots, s_n) = 0$, y como el anillo $A[X_1, \ldots, X_n]$ es íntegro (teorema 1', § 2 del cap. 5), entonces, de aquí se deduce la igualdad $h(s_1, \ldots, s_n) = 0$. Esto, sin embargo, es imposible, por cuanto $\deg h(Y_1, \ldots, Y_n) = \deg g(Y_1, \ldots, Y_n) - 1$. Por lo tanto, $g_0 \neq 0$. Examinando ahora la identidad

$$g_0(s_1, \ldots, s_{n-1}) + \ldots + g_k(s_1, \ldots, s_{n-1}) s_n^k = g(s_1, \ldots, s_n) = 0$$

en $A[X_1, \ldots, X_n]$, sustituyamos X_n por 0. Entonces, todos los términos, excepto el primero, se reducirán a cero, y obtendremos

$$g_0((s_1)_0, \ldots, (s_{n-1})_0) = 0,$$

donde $(s_1)_0, \ldots, (s_{n-1})_0$ son polinomios simétricos elementales en las variables $X_1, \ldots, X_{n-1}$ (véase (3)). Ellos, por presupuesto de la inducción, son algebraicamente independientes sobre A. Al mismo tiempo, tenemos $g_0 \neq 0$. La contradicción obtenida concluye la demostración de unicidad, y, junto con ella, la de todo el teorema 1. ∎

Notemos, que la demostración de la primer parte del teorema fue constructiva, y ella puede ser utilizada para la búsqueda práctica del polinomio g. Además, de los razonamientos se deduce, que los coeficientes del polinomio buscado g se encuentran en un subanillo del anillo A, engendrado por los coeficientes de polinomio f dado. En particular, para $A = \mathbb{Z}$ los coeficientes de los polinomios f y g serán números enteros.

COROLARIO. *Sea $f(X) = X^n + a_1 X^{n-1} + \ldots + a_{n-1} X + a_n$ un polinomio unitario de grado n en una variable X sobre el campo P, que tiene n raíces $c_1, \ldots, c_n$ en algún campo mayor $F \supset P$. Sea, luego, $h(X_1, \ldots, X_n)$ un polinomio simétrico cualquiera de $P[X_1, \ldots, X_n]$. Entonces, su valor $h(c_1, \ldots, c_n)$, obtenido al sustituir X_i por c_i, $i = 1, \ldots, n$, pertenecerá al campo P.*

DEMOSTRACION. De hecho, por el teorema fundamental sobre los polinomios simétricos, existe un polinomio $g(Y_1, \ldots, Y_n) \in$ $\in P[Y_1, \ldots, Y_n]$ tal, que $h(X_1, \ldots, X_n) = g(s_1(X_1, \ldots, X_n) \ldots$ $\ldots, s_n(X_1, \ldots, X_n))$. Por eso, $h(c_1, \ldots, c_n) = g(s_1(c_1, \ldots$

$\ldots, c_n), \ldots, s_n(c_1, \ldots, c_n))$, y puesto que, de acuerdo con las formulas de Viete (12) § 1, $s_k(c_1, \ldots, c_n) = (-1)^k a_k \in P$, entonces, también $g(-a_1, \ldots, (-1)^n a_n) \in P$. ■

3. Método de los coeficientes indeterminados. Existen varias demostraciones distintas del teorema fundamental sobre los polinomios simétricos, y, respectivamente, distintos métodos de expresión del polinomio f dado, por medio de polinomios simétricos elementales. A fin de describir uno de los métodos más usados, introduzcamos un nuevo tipo de polinomio simétrico. Para precisión tomaremos en calidad de A el anillo $\mathbb{Z}$ o el campo $\mathbb{R}$. Sea $v = X_1^{i_1} \ldots X_n^{i_n}$ algún monomio. Convengamos en llamar a v *monomio monótono*, si $i_1 \geq i_2 \geq \ldots \geq i_n$. Designemos con $S(v)$ la suma de todos los distintos monomios de la familia de $n!$ monomios del tipo πv, $\pi \in S_n$. Expresándolo de otro modo,

$$S(v) = \sum_{\pi \in S_n/H} \pi v,$$

donde la condición $\pi \in S_n/H$ significa que π recorre el conjunto de los representantes de las clases adjuntas a la izquierda de πH de grupo S_n por el subgrupo $H = \{\tau \in S_n \mid \tau v = v\}$ (corresponde realizar la sencilla comprobación de que el subconjunto H, determinado de este modo, realmente es un subgrupo). Por ejemplo,

$$p_k(X_1, \ldots, X_n) = S(X_n^k) = X_1^k + X_2^k + \ldots + X_n^k, \quad k \geq 0, \qquad (6)$$

es la llamada *suma de potencias*. Aquí, evidentemente, $H = S_{n-1}$. Luego, $S(X_1 X_2 \ldots X_k) = s_k(X_1, \ldots, X_n)$ (¿con qué coincide aquí H?). Es claro, que $S(v)$ es un polinomio simétrico homogéneo de un mismo grado total que v. Como $S(v) = S(\sigma v)$, $\forall \sigma \in S_n$, entonces, es natural considerar solamente las sumas $S(v)$ con monomios monótonos v. Por el sentido, es claro también que cualquier polinomio simétrico f sobre A, es una combinación lineal, con coeficientes de A, de polinomios del tipo $S(v)$:

$$f = \sum a_v S(v).$$

Habitualmente, esta escritura se obtiene inmediatamente («a ojo»). De este modo, la tarea se reduce a la expresión de $S(v)$ por medio de polinomios simétricos elementales.

Convengamos en disponer los monomios en $S(v)$ en forma *lexicográfico* (por el principio de ordenación de los diccionarios), o sea, de tal manera, que el monomio $v = X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$ antecede al monomio (o, es mayor que el monomio) $w = X_1^{j_1} X_2^{j_2} \ldots X_n^{j_n}$ $(v > w)$ exactamente entonces, cuando la sucesión $i_1 - j_1$, $i_2 - j_2$, $\ldots, i_n - j_n$ tiene la forma $0, \ldots, 0, t, \ldots$, donde $t > 0$ (a la derecha de t pueden haber diferencias negativas $i_l - j_l$). Naturalmente, el principio lexicográfico de ordenamiento de los términos se puede aplicar no sólo con respecto a $S(v)$, sino que a cualquier polinomio $f \in A[X_1, \ldots, X_n]$. En el sentido lexicográfico, el término

superior (o *primero*) de la suma $S(v)$ con monomio monótono v, será v. Para el monomio monótono $v = X_1^{i_1}X_2^{i_2}\ldots X_n^{i_n}$ tenemos derecho a considerar el producto

$$g_v = s_1^{i_1-i_2}s_2^{i_2-i_3}\ldots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}, \quad s_i = s_i(X_1, \ldots, X_n), \tag{7}$$

en el cual el término superior resultará una vez más

$$v = X_1^{i_1-i_2}(X_1X_2)^{i_2-i_3}\ldots(X_1\ldots X_{n-1})^{i_{n-1}-i_n}(X_1\ldots X_n)^{i_n}$$

(a fin de obtener el término superior en el producto, hay que tomar el término superior en cada uno de los factores). De aquí se deduce, que el término superior de la diferencia $S(v) - g_v$, será menor que v. En consecuencia,

$$S(v) - g_v = \sum n'_w S(w),$$

donde $n'_w \in \mathbb{Z}$, y la suma se realiza por el conjunto de los monomios monótonos $w \prec v$. Las potencias totales de v y de todas las w coinciden.

Ahora se diseña el método siguiente de expresión de $S(v)$ por medio de polinomios simétricos elementales. Sea $\deg v = m$. Se toman todas las particiones «monótonas»

$$m = j_1 + j_2 + \ldots + j_n, \; j_1 \geqslant j_2 \geqslant \ldots \geqslant j_n \geqslant 0,$$

del número entero m, tales, que $w = X_1^{j_1}X_2^{j_2}\ldots X_n^{j_n} < v$. Se examina el conjunto M_v de la totalidad de tales monomios w. Para cada $w \in M_v$ se conforma el monomio g_w (véase (7)). Ya sabemos, que

$$S(v) = g_v + \sum_{w \in M_v} n_w g_w, \tag{8}$$

donde n_w son ciertos números enteros. Los coeficientes indeterminados n_w (y de ahí el nombre: ***método de los coeficientes indeterminados***) se encuentran sustituyendo sucesivamente $X_1, \ldots, X_n$ en (8) por algunos números enteros, habitualmente, ceros y unidades. Los valores de g_v, g_w y $S(v)$ son dados, y para n_w se obtiene, notoriamente, un sistema común de ecuaciones lineales.

EJEMPLO. $v = X_1^3$, $S(v) = p_3(X_1, \ldots, X_n)$, $n \geqslant 3$, $g_v = s_1^3$,

M_v	$X_1^2X_2$	$X_1X_2X_3$
g_w	s_1s_2	s_3

En este caso, la ecuación (8) tiene la forma

$$p_3 = s_1^3 + as_1s_2 + bs_3.$$

Si $X_1 = X_2 = 1$, $X_i = 0$ para $i > 2$, entonces, $p_3 = 2$, $s_1 = 2$, $s_2 = 1$, $s_3 = 0$. Y, si $X_1 = X_2 = X_3 = 1$, $X_i = 0$ para $i > 3$, entonces, $p_3 = 3$,

$s_1 = 3$, $s_2 = 3$, $s_3 = 1$. Del sistema obtenido

$$2 = 2^3 + a\cdot 2\cdot 1 + b\cdot 0,$$
$$3 = 3^3 + a\cdot 3\cdot 3 + b\cdot 1,$$

hallamos $a = -3$, $b = 3$, o sea, $p_3 = s_1^3 - 3s_1s_2 + 3s_3$.

Para la expresión de las sumas de potencias $p_k(X_1, \ldots, X_n)$ en forma de polinomios en $s_1, s_2, \ldots, s_n$ se tienen fórmulas más cómodas, llamadas *fórmulas de Newton*:

$$p_k - p_{k-1}s_1 + p_{k-2}s_2 + \ldots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k = 0$$

para $1 \leqslant k \leqslant n$; (9)

$$p_k - p_{k-1}s_1 + p_{k-2}s_2 + \ldots + (-1)^{n-1} p_{k-n+1}s_{n-1} + (-1)^n p_{k-n}s_n = 0 \qquad (10)$$

para $k > n$.

A fin de demostrarlas, utilicemos las evidentes relaciones

$$X_i^n - s_1X_i^{n-1} + \ldots + (-1)^{n-1}s_{n-1}X_i + (-1)^n s_n = 0,$$

que se obtienen al sustituir $Y = X_i$ en (3). Multiplicando cada una de estas relaciones por X_i^{k-n} $(k \geqslant n)$:

$$X_i^k - s_1X_i^{k-1} + \ldots + (-1)^{n-1}s_{n-1}X_i^{k-n+1} + (-1)^n s_n X_i^{k-n} = 0$$

y efectuando luego la suma por i de 1 a n, obtenemos no sólo la fórmula (10), sino que también la fórmula (9) para $k = n$ $(p_0 = X_1^0 + \ldots + X_n^0 = n)$. Examinemos, luego, el polinomio homogéneo simétrico $f_{k,n}$ de grado $k \leqslant n$ $(0 = -\infty$, si $f_{k,n} = 0)$:

$$f_{k,n}(X_1, \ldots, X_n) = p_k - p_{k-1}s_1 + \ldots$$
$$\ldots + (-1)^{k-1} p_1 s_{k-1} + \ldots + (-1)^k k s_k.$$

Utilizando la inducción en $r = n - k$, demostremos que $f_{k,n}$ es idénticamente igual a cero. Para $r = 0$, este hecho se acaba de establecer. Haciendo $X_n = 0$ y observando que los así obtenidos polinomios simétricos $(s_i)_0$, $(p_i)_0$ coinciden con los polinomios s_i y p_i, determinados para las $n - 1$ variables $X_1, \ldots, X_{n-1}$ (véanse (3) y (6)), llegamos a la igualdad

$$f_{k,n}(X_1, \ldots, X_{n-1}, 0) =$$
$$= (p_k)_0 - (p_{k-1})_0 (s_1)_0 + \ldots + (-1)^{k-1} (p_1)_0 (s_{k-1})_0 +$$
$$+ (-1)^k k (s_k)_0 = f_{k,n-1}(X_1, \ldots, X_{n-1}) = 0,$$

pues, $n - 1 - k = r - 1 < r$, y es aplicable el presupuesto de la inducción.

La relación $f_{k,n}(X_1, \ldots, X_{n-1}, 0) = 0$ muestra que el polinomio $f_{k,n}$ se divide por X_n: $f_{k,n} = X_n f_1$. Utilizando la simetría

de $f_{k,n}$ (véase el correspondiente razonamiento en la demostración de la primera parte del teorema 1), obtenemos

$$f_{k,n}(X_1, \ldots, X_n) = s_n(X_1, \ldots, X_n)\, g(X_1, \ldots, X_n),$$

lo que es posible, sin embargo, sólo cuando $g = 0$, por cuanto $\deg s_n = n$, y $\deg f_{k,n} = k < n$. Y bien, $f_{k,n} = 0$, y la demostración de la fórmula (9) ha concluido.

4. Discriminante de un polinomio. En el anillo $P[X_1, \ldots, X_n]$, examinemos el polinomio

$$\Delta_n = \prod_{1 \leqslant j < i \leqslant n} (X_i - X_j),$$

el que, evidentemente, se puede presentar en forma de determinante de Vandermonde

$$\Delta_n = \begin{vmatrix} 1 & 1 & & 1 \\ X_1 & X_2 & & X_n \\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & & \cdot\ \cdot\ \cdot \\ X_1^{n-1} & X_2^{n-2} & \ldots & X_n^{n-1} \end{vmatrix} \qquad (11)$$

Como el determinante es una función antisimétrica de sus columnas, entonces, $\pi(\Delta_n) = \varepsilon_\pi \Delta_n$ es el signo de permutación $\pi \in S_n$. Pero, en tal caso, Δ_n^2 es un polinomio simétrico y, por el teorema fundamental, él puede ser expresado en forma de un polinomio en funciones simétricas elementales

$$\Delta_n^2 = \prod (X_i - X_j)^2 = \mathrm{Dis}(s_1, \ldots, s_n).$$

El polinomio Dis en $s_1(X_1, \ldots, X_n), \ldots, s_n(X_1, \ldots, X_n)$ se llama *discriminante de la familia* $X_1, \ldots, X_n$. Sus coeficientes, evidentemente, pertenecen a $\mathbb{Z}$. Al sustituir X_i por $x_i \in F$, $i = 1, 2, \ldots, n$ (F es alguna ampliación del campo P), se puede hablar del discriminante de una familia de culesquiera n elementos del campo F. Si no todos los $x_1, \ldots, x_n \in F$ son distintos, entonces, el discriminante de esta familia se reduce a cero, por cuanto, por lo menos uno de los factores $x_i - x_j$ será igual a cero. La propiedad del Dis de separar este caso explica el propio término discriminante.

Un método cómodo de obtención del discriminante se basa en la interpretación de Δ_n^2 como el producto del determinante (11) por el determinante transpuesto: $\Delta_n^2 = \Delta_n^t \Delta_n$ (recordemos, que $\det {}^tA = \det A$, para cualquier matriz cuadrada A).

Operando de acuerdo con la regla de multiplicación de matrices, inmediatamente hallamos

$$\mathrm{Dis}(s_1, \ldots, s_n) = \begin{vmatrix} n & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ p_2 & p_3 & p_4 & \cdots & p_{n-1} \\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{vmatrix} \qquad (12)$$

donde p_k son las sumas de potencias (6) conocidas por nosotros. Calculando p_k por las fórmulas recurrentes (9) y (10), llegamos a la expresión explícita de $\text{Dis}(s_1, \ldots, s_n)$. En particular, $p_1 = s_1$, $p_2 = s_1^2 - 2s_2$, así que

$$\text{Dis}(s_1, \ldots, s_2) = \begin{vmatrix} 2 & s_1 \\ s_1 & s_1^2 - 2s_2 \end{vmatrix} = s_1^2 - 4s_2. \qquad (13)$$

Sea nos dado ahora el polinomio unitario

$$f(X) = X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in P[X],$$

que tiene en P, o en alguna ampliación del mismo F, n raíces $c_1, \ldots, c_n$. Como sabemos de las fórmulas de Viete, $a_k = (-1)^k s_k \times (c_1, \ldots, c_n)$.

DEFINICION. El discriminante de la familia de raíces $c_1, \ldots, c_n$ del polinomio f, o lo que es equivalente, el valor del discriminante $\text{Dis}(s_1, \ldots, s_n)$, obtenido al sustituir s_k por $(-1)^k a_k$, se llama *discriminante del polinomio* f y se designa con el símbolo $D(f)$. Se llama también *discriminante de la ecuación algebraica*

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0. \qquad (14)$$

Es claro, que $D(f) \in P$ (recordemos, en relación con esto, el corolario del teorema 1). Como se ve de la definición de discriminante, es también legítima la

PROPOSICION. D $(f) = 0$ *si, y sólo si, la ecuación* (14) *tiene raíces múltiples (por lo menos una raíz de multiplicidad* $k > 1$). ∎

Teniendo en cuenta el corolario 2 del teorema 5 del § 1, tenemos ahora dos métodos, que no requieren salir fuera de los límites del campo fundamental P, para resolver si tiene o no el polinomio : $f \in P[X]$ raíces múltiples. Pero, la importancia del discriminante no se reduce sólo a esto. Digamos, la fórmula (13), aplicada al trinomio cuadrado $f(x) = X^2 + aX + b$ con coeficientes reales a, b, da D $(f) = a^2 - 4b$, expresión conocida del álgebra elemental. En particular, del signo del D (f) depende el que las raíces de la ecuación $x^2 + ax + b = 0$ sean reales o complejas conjugadas.

En calidad de ejemplo calculemos también el discriminante de la llamada ecuación cúbica incompleta

$$f(x) = x^3 + ax + b = 0 \qquad (15)$$

En el caso dado $s_4 = 0$ y el cálculo de p_k por las fórmulas recurrentes da $p_1 = s_1 = 0$, $p_2 = s_1^2 - 2s_2 = -2a$, $p_3 = s_1^3 - 3s_1s_2 + 3s_3 = -3b$, $p_4 = s_1^4 - 4s_1^2s_2 + 4s_1s_3 + 2s_2^2 = 2a^2$. Por lo tanto, por la fórmula (12) tenemos

$$D(f) = \begin{vmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{vmatrix} = -4a^3 - 27b^2. \qquad (16)$$

La expresión de $D(f)$ adquiere un aspecto más complejo (en comparación con (16)) en el caso de la ecuación cúbica completa $x^3 + a_1x^2 + a_2x + a_3 = 0$, sin

embargo, uno puede liberarse de su examen, tal como lo muestra el siguiente razonamiento general.

Pasemos del argumento x a $y = x - \frac{a_1}{n}$. Sustituyendo $x = y - \frac{a_1}{n}$ en la ecuación (14)), y usando la fórmula binomial, hallamos, que

$$g(y) = f\left(y - \frac{a_1}{n}\right) = y^n + a y^{n-2} + \ldots = 0, \qquad (17)$$

o sea, en la nueva ecuación el coeficiente de y^{n-1} es igual a cero. Conociendo la raíz y_0 de la ecuación (17), hallamos fácilmente también la raíz $x_0 = y_0 - \frac{a_1}{n}$ de la ecuación original (14). Por eso, sin limitación de generalidad se puede considerar que $a_1 = 0$.

Si se intenta hallar una fórmula general para la resolución de la ecuación (15) (lo que lograron los matemáticos medievales Escipión del Ferro, Cardan y otros), entonces, obligatoriamente, el discriminante (16) entrará en juego (véanse las fórmulas (2), § 2 del cap. 1).

5. Resultante. La propiedad fundamental de D(f), formulada en la proposición del punto anterior, también se interpreta como criterio de existencia de raíces comunes (o de multiplicadores comunes) en el polinomio f y su derivada f'. En la base de este criterio se encuentra, al fin de cuentas, el algoritmo de Euclides. Esto da motivo para suponer, que se tiene un criterio análogo que permite, en base a los coeficientes de dos polinomios cualesquiera $f, g \in P[X]$, resolver inmediatamente la cuestión de si tienen o no estos polinomios multiplicadores comunes. Y bien, sean

$$f(X) = a_0X^n + a_1P^{n-1} + \ldots + a_{n-1}X + a_n,$$
$$g(X) = b_0X^m + b_1X^{n-1} + \ldots + b_{m-1}X + b_m$$

dos polinomios con coeficientes en el campo P. Aquí $n > 0$, $m > 0$, pero no se excluye la posibilidad de que $a_0 = 0$ o bien $b_0 = 0$.

DEFINICION. Se llama *resultante* Res (f, g) de los polinomios f y g, el polinomio homogéneo (función polinómica homogénea) de sus coeficientes (de grado m con respecto a $a_0, \ldots, a_n$, y de grado n con respecto a $b_0, \ldots, b_m$) del tipo

$$\mathrm{Res}(f, g) = \left|\begin{matrix} a_0 & a_1 & \ldots & a_n & & & \\ & a_0 & a_1 & \ldots & a_n & & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ & & & a_0 & a_1 & \ldots & a_n \\ b_0 & b_1 & \ldots & b_m & & & \\ & b_0 & b_1 & \ldots & b_m & & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ & & & b_0 & b_1 & \ldots & b_m \end{matrix}\right| \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ filas} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ filas} \end{matrix}$$

Esta definición de resultante contiene cierta afirmación acerca de los grados de ella como polinomio. Pero esta afirmación se deriva

inmediatamente de las propiedades de los determinantes: si se sustituye en las primeras m filas a_i por ta_i, entonces, Res $(tf, g) = t^m$ Res (f, g), después de lo cual queda por referirse al ejercicio 3 del § 2 del cap. 5.

Deduzcamos ahora las principales propiedades de la resultante.

Res 1. Res $(f, g) = 0$ *si, y sólo si,* $a_0 = 0 = b_0$, *o si* f *y* g *tienen multiplicadores comunes en* $P[X]$ *de grado* > 0.

Convencémonos al principio de que la condición «$a_0 = 0 = b_0$, o que f y g tienen multiplicadores comunes en $P[X]$ de grado > 0» se cumple si, y sólo si, existen los polinomios f_1, g_1 no iguales a cero al mismo tiempo para los cuales,

$$fg_1 + f_1g = 0, \quad \deg f_1 < n, \quad \deg g_1 < m. \tag{18}$$

Efectivamente, sea $h =$ m.c.d. (f, g), $\deg h > 0$. Entonces, $f = hf_1$, $g = -hg_1$ y, en consecuencia, $fg_1 + gf_1 = 0$. Además, $\deg f_1 < n$, $\deg g_1 < m$, así que tiene lugar (18). Para $a_0 = 0 = b_0$ podemos hacer $f_1 = f$, $g_1 = -g$.

A la inversa, suponiendo con el cumplimiento de (18), que m.c.d. $(f, g) = 1$, en virtud de la factorizabilidad de $P[X]$ (véase el § 3 del cap. 5) llegamos a la implicación $fg_1 = -gf_1 \Rightarrow f \mid f_1$, $g \mid g_1$. Así que, $\deg f < n$, $\deg g < m$, de donde $a_0 = 0 = b_0$.

Demostremos ahora la equivalencia de las condiciones (18) y Res $(f, g) = 0$. Haciendo

$$f_1 = c_0X^{n-1} + c_1X^{n-2} + \ldots + c_{n-1},$$
$$g_1 = d_0X_m^{-1} + c_1X_m^{-2} + \ldots + d_{m-1}$$

y calculando, por las reglas formales los coeficientes del polinomio $fg_1 + f_1g$ de grado $\leqslant n + m - 1$, escribimos la condición (18) en forma de un sistema cuadrado homogéneo de ecuaciones lineales con $(n + m)$ incógnitas $d_0, d_1, \ldots, d_{m-1}, c_0, c_1, \ldots, c_{n-1}$:

$$\begin{aligned} a_0d_0 + \ldots + b_0c_0 &= 0, \\ a_1d_0 + a_0d_1 + \ldots + b_1c_0 + b_0c_1 &= 0, \\ a_2d_0 + a_1d_1 + a_0d_2 + \ldots + b_2c_0 + b_1c_1 + b_0c_2 &= 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \tag{19}$$

El determinante de la matriz del sistema (19) (más exactamente, el determinante de la matriz transpuesta) precisamente coincide con Res (f, g). Por consiguiente, el sistema (19) tiene solución no nula exactamente entonces, cuando Res $(f, g) = 0$, y cualquier solución no nula lleva al par de polinomios f_1, g_1, que cumplen la condición (18). ∎

Res 2. *Sea que los polinomios* f *y* g *se desagregan totalmente en multiplicadores lineales en* $P[X]$:

$$f(X) = a_0(X - \alpha_1) \ldots (X - \alpha_n),$$
$$g(X) = b_0(X - \beta_1) \ldots (X - \beta_m).$$

Entonces

$$\operatorname{Res}(f, g) = a_0^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j) = a_0^m b_0^n \prod_{i,j} (\alpha_i - \beta_j).$$

DEMOSTRACION Es claro, que las fórmulas aquí indicadas, si son correctas, deberán tener carácter universal, independiente de los tipos particulares de polinomios f, g. Esta sencilla «filosofía», en cuya naturaleza no queremos aquí entrar, nos permite limitarnos a la consideración del «caso general» cuando, digamos, todos $g(\alpha_1), \ldots, g(\alpha_n)$ y todos $f(\beta_1), \ldots, f(\beta_m)$ son distintos de dos en dos.

Luego, como $\operatorname{Res}(g, f) = (-1)^{mn} \operatorname{Res}(f, g)$ (véase la definición), entonces, es suficiente convencerse de la veracidad de la relación $\operatorname{Res}(f, g) = a_0^m \prod g(\alpha_i)$. Con este fin introducimos una nueva variable Y y sobre el campo de las fracciones racionales $P(Y)$ consideremos los polinomios $f(X)$ y $g(X) - Y$. De la definición de resultante, donde hay que sustituir b_m por $b_m - Y$, se obtiene que

$$\operatorname{Res}(f, g - Y) = (-1)^n a^m Y^n + \ldots + \operatorname{Res}(f, g)$$

es un polinomio de grado n con relación a Y con coeficiente superior $(-1)^n a_0^m$ y con término independiente $\operatorname{Res}(f, g)$. Los polinomios $f(X)$ y $g(X) - g(\alpha_i)$ con la raíz común α_i son divisibles por $X - \alpha_i$. En virtud de la propiedad Res 1, tenemos $\operatorname{Res}(f, g - g(\alpha_i)) = 0$.

Por el teorema de Bezout, el polinomio $\operatorname{Res}(f, g - Y)$ debe ser divisible por $g(\alpha_i) - Y$, $1 \leqslant i \leqslant n$. Como todos los $g(\alpha_i)$ son distintos, entonces, $\operatorname{Res}(f, g - Y) = a_0^m \prod_{i=1}^{n} (g(\alpha_i) - Y)$. Para $Y = 0$ obtenemos la expresión necesaria.

Traslademos la definición de discriminantes, dada en el punto 4, al caso de polinomios no unitarios, haciendo

$$D(f) = a_0^{2n-2} \prod_{1 \leqslant j < i \leqslant n} (\alpha_i - \alpha_j)^2 = [a_0^{n-1} \prod_{j<i} (\alpha_i - \alpha_j)]^2, \quad a_0 \neq 0.$$

Res 3. *Tiene lugar la fórmula*

$$D(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{-1} \operatorname{Res}(f, f'). \tag{20}$$

Efectivamente, de acuerdo con Res 2,

$$\operatorname{Res}(f, f') = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i).$$

Pero

$$f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j),$$

que es una consecuencia sencilla de la sustitución $X = \alpha_i$ en la expresión general

$$f'(X) = a_0 \sum_{j=1}^{n} \prod_{j \neq i} (X - \alpha_j),$$

obtenida por la diferenciación del producto $f(X) = a_0 \prod_{j=1}^{n} (X - \alpha_j)$ De esto modo,

$$\mathrm{Res}(f, f') = a_0^{2n-1} \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j) =$$

$$= a_0 (-1)^{\frac{n(n-1)}{2}} a_0^{2n-2} \prod_{j<i} (\alpha_i - \alpha_j)^2 = a_0 (-1)^{\frac{n(n-1)}{2}} D(f). \quad ■$$

La fórmula (20) brinda una expresión explícita para el discriminante.

EJERCICIOS

1. Con ayuda de las fórmulas de Newton (9), (10), mostrar, que

$$\sum_{i=1}^{p-1} i^m = \begin{cases} -1 \pmod p, \text{ si } m \text{ se divide por } p-1, \\ 0 \pmod p, \text{ si } m \text{ no se divide por } p-1. \end{cases}$$

2. Sean, c_1, c_2, c_3, raíces complejas del polinomio $X^3 - X + 1$. ¿Qué se puede decir sobre la ampliación $\mathbb{Q}(c_1^{89} + c_2^{89} + c_3^{89})$?

3. El polinomio $f(X_1, \ldots, X_n)$ sobre el campo P, de característica $\neq 2$, se llama *antisimétrico (o alternativo)*, si $(\pi f)(X_1, \ldots, X_n) = e_\pi f(X_1, \ldots, X_n)$, $\forall \pi \in S_n$ (como siempre, e_π es el signo de la permutación). Como ejemplo de polinomio antisimétrico, puede servir $\Delta_n = \prod_{j>i} (X_i - X_j)$. Mostrar, que cualquier polinomio antisimétrico $f \in P[X_1, \ldots, X_n]$ tiene la forma $f = \Delta_n \cdot g$, donde g es un polinomio simétrico. (*Indicación.* Considerar f fomo un polinomio con relación a X_n con coeficientes en $P[X_1, \ldots, X_{n-1}]$. Prestar atención a que, en virtud de la antisimetría $f = 0$ cuando $X_n = X_{n-1}$ y, en consecuencia, f es divisible por $X_n - X_{n-1}$).

4. Usando la propiedad Res 2 y el hecho de la existencia del campo de descomposición de un polinomio (véase el teorema 2 en el parágrafo siguiente), mostrar que

$$\mathrm{Res}(fg, h) = \mathrm{Res}(f, h) \cdot \mathrm{Res}(g, h).$$

5. Del ejercicio 4 y de Res 3, deducir la fórmula:

$$D(fg) = D(f) D(g) [\mathrm{Res}(f, g)]^2.$$

6. ¿A qué es igual la resultante $\mathrm{Res}(f(X), X - 1)$?

7. Mostrar que $D(X^n + a) = (-1)^{\frac{n(n-1)}{2}} n^n a^{n-1}$.

8. Sea $f(X) = X^{n-1} + X^{n-2} + \ldots + 1$. Empleando la relación $X^n - 1 = (X - 1) f(X)$ y el ejercicio anterior, mostrar que $D(f) = (-1)^{\frac{(n-1)(n-2)}{2}} \times n^{n-2}$.

§ 3. CIERRE ALGEBRAICO DEL CAMPO C

1. Formulación del teorema fundamental. Sean, P un campo y f un polinomio arbitrario sobre P. Como ya se indicó en el punto 2 del § 1, la conducta de la función polinómica $\tilde{f}\colon P \to P$, asociada con f, depende esencialmente del campo P. En particular, $\operatorname{Im} \tilde{f} = P$, si, en cuanto $\deg f > 0$ y con respecto a P es aplicable la siguiente

DEFINICION El campo P se llama *algebraicamente cerrado*, si cada polinomio del anillo $P[X]$ se descompone en factores lineales.

Esto mismo se puede expresar con otras palabras: *El campo P es algebraicamente cerrado, si son irreducibles sobre P solamente los polinomios de grado 1 (polinomios lineales).*

Si cualquier polinomio $f \in P[X]$ tiene en P por lo menos una raíz, entoces, el campo P es algebraicamente cerrado. Efectivamente, entonces $f(X) = (X - a)\, h(X)$, $a \in P$, $h \in P[X]$, pero, por condición, para el polinomio h en P también existe, por lo menos, una raíz, o sea, $h(X) = (X - b)\, r(X)$, $b \in P$, $r \in P[X]$. Continuando este proceso, llegamos al fin de cuentas a una descomposición total de f en factores lineales. Como f es un polinomio arbitrario, entonces, el campo P satisface la definición de cierre algebraico.

Aunque es legítima la afirmación de que, para todo campo P existe una ampliación $\tilde{P} \supset P$, que es un campo algebraicamente cerrado (*teorema de Steinits*), en un principio no sólo es difícil comprender la construcción de una ampliación algebraicamente cerrada, sino que también la propia idea de tal ampliación. Por eso es más grato, que disponemos, de hecho, de un ejemplo claro y muy importante de campo algebraico cerrado, tal como lo dice el llamado «teorema fundamental del álgebra». Precisamente, es correcto el

TEOREMA 1. *El campo de los números complejos* $\mathbb{C}$ *es algebraicamente cerrado.*

Formulemos de nuevo esta afirmación fundamental, ahora ya en términos de raíces:

Un polinomio arbitrario $f(X)$ de grado $n \geqslant 1$ con coeficientes complejos (o reales), tiene exactamente n raíces complejas, teniendo en cuenta sus multiplicidades.

El elevado título de «fundamental» el teorema 1 lo obtuvo ya en los tiempos cuando la resolución de ecuaciones algebraicas era una de las principales ocupaciones de los algebraistas. En nuestros días, el teorema 1 es una de las afirmaciones ordinarias, aunque importantes.

Por primera vez la demostración rigurosa del «teorema fundamental» fue propuesta por Gauss en 1799. Desde entonces, han aparecido muchas variantes de demostración, que se distinguen entre sí, digamos, por el grado de su algebraicidad. La necesidad de apoyarse en las propiedades de continuidad de los campos $\mathbb{R}$ y $\mathbb{C}$ (de otro modo:

en la topología de los mismos) se manifiesta de una u otra forma; existe incluso una demostración muy breve no algebraica, basada en el relativamente profundo concepto de función analítica de variable compleja. A continuación se expone una demostración que, por su espíritu, es la más algebraica de todas las accesibles a nosotros. Lo más natural sería quizás, una demostración que utilizase los medios de la teoría de Galois, pero nos limitaremos a esta breve mención.

La parte no algebraica de la demostración del teorema 1, se reduce a los dos lemas siguientes.

LEMA 1. (sobre el módulo del término superior). *Sea*

$$f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \tag{1}$$

un polinomio de grado $n \geqslant 1$ con coeficientes complejos arbitrarios. Entonces, para la aplicación polinómica $z \to f(z)$ del campo C *en sí mismo, se puede indicar un número positivo $r \in \mathbb{R}$ tal, que para $|z| > r$ se cumplirá la desigualdad*

$$|a_0z^n| > |a_1z^{n-1} + \ldots + a_{n-1}z + a_n|.$$

DEMOSTRACION. Hagamos $A = \max(|a_1|, \ldots, |a_n|)$ y $r = \frac{A}{|a_0|} + 1$. Si se toma $|z| > r \geqslant 1$, entonces, obtenemos $|a_0| > \frac{A}{|z|-1}$, de donde, de acuerdo con las reglas de las operaciones con los módulos de los números complejos (véase el § 1 del cap. 5), tendremos,

$$|a_0z^n| = |a_0|\,|z|^n > \frac{A\,|z|^n}{|z|-1} > \frac{A\,(|z|^n-1)}{|z|-1} =$$

$$= A(|z|^{n-1} + \ldots + |z| + 1) \geqslant |a_1|\,|z|^{n-1} + \ldots + |a_{n-1}|\,|z| + |a_n| +$$

$$= |a_1z^{n-1}| + \ldots + |a_{n-1}z| + |a_n| \geqslant |a_1z^{n-1} + \ldots + a_{n-1}z + a_n|. \quad \blacksquare$$

COROLARIO. *Sea que el polinomio (1) de grado $n \geqslant 1$ tiene coeficientes reales. Entonces, para todos los valores de $x \in \mathbb{R}$, suficientemente grandes por su valor absoluto, el signo (del número real) $f(x)$ coincide con el signo del «término superior» a_0x^n.* $\blacksquare$

LEMA 2. *El polinomio de grado impar con coeficientes reales tiene, por lo menos, una raíz real.*

DEMOSTRACION. En virtud de que n es impar, el término superior a_0x^n de la aplicación polinomial $\tilde{f}\colon \mathbb{R} \to \mathbb{R}$ tendrá distintos signos, según sean positivos o negativos los valores de $x \in \mathbb{R}$. Tomando estos valores de x lo suficientemente grandes, por sus magnitudes absolutas, podemos afirmar, de acuerdo con el corolario del lema 1, que también $f(x)$ tendrá distintos signos. Si, por ejemplo, $a_0 > 0$, entonces, $f(-r) < 0$, y $f(r) > 0$, donde r es un número real, tomado de la demostración del lema 1. Del curso de análisis mate-

mático es sabido (y esto no es difícil de demostrarlo inmediatamente), que la aplicación polinomial $\tilde{f}$ es continua (de otro modo: la función racional entera $x \mapsto f((x)$, es continua). La función continua f tiene la propiedad de tomar, en el intervalo $-r \leqslant x \leqslant r$, cualquier valor intermedio entre $f(-r)$ y $f(r)$. En particular, para algún c con $|c| \leqslant r$ será $f(c) = 0$. El mismo razonamiento sirve para $a_0 < 0$. ∎

Con esta afirmación geométrica e intuitivamente clara, nuestros razonamientos algebraicos concluyen. La etapa siguiente la llevaremos a cabo en un contexto que no tiene relación directa con $\mathbb{C}$, y presentaremos una estructura que es interesante por sí misma.

2. Campo de descomposición de un polinomio. Como frecuentemente sucede, una «mirada desde afuera» a un jemplo muy conocido, brinda la posibilidad de comprenderlo mejor y de pasar a generalizaciones razonables. Recordemos la realización del campo $\mathbb{C}$ en forma de anillo cociente $\mathbb{R}[x]/(x^2+1)\,\mathbb{R}[X]$ (teorema 6, § 2 del cap. 5). Sustituyendo aquí R por el campo arbitrario P, y X^2+1 por cualquier polinomio $f \in P[X]$, llegamos al «anillo de clases de restos por el módulo (f)» o, lo que es lo mismo, al anillo cociente $P[X]/(f)$, donde $(f) = f \cdot P[X]$ es un ideal en $P[X]$. El ideal (f) está compuesto de todos los polinomios divisibles por f y es, de acuerdo con el corolario del teorema 5 del § 2 del cap. 5, el ideal más general en $P[X]$. La analogía entre los anillos $\mathbb{Z}$ y $P(X]$ se hace extensible a los correspondientes anillos de las clases de restos $Z_n = \mathbb{Z}/(n)$ y $P[X]/(f)$. Es útil repetir las principales etapas de la construcción de Z_n en el § 4 del cap. 4.

Sirven de elementos del anillo cociente $P[X]/(f)$ las clases de restos $\tilde{g} = g + (f)$, cada una de las cuales puede ser expresada en la formar $r + (f)$, donde $\deg r < \deg f$. Como en el caso de $\mathbb{Z}$, sirve de demostración la misma división con resto: si $g = gf + r$, entonces, $g + (f) = r + gf + (f) = r + (f)$, por cuanto $qf \in (f)$. Es fácil observar que los elementos $\bar{a}$, $a \in P$, forman en $P[X]/(f)$ un subanillo isomorfo al campo P. Luego, la reducibilidad del polinomio f sobre P, o sea, la posibilidad de escribirlo en forma de $f = f_1 f_2$, donde $f_i \in P[X]$ y $0 < \deg f_i < \deg f$, implica la existencia de divisores no triviales de cero en $P[X]/(f)$; precisamente, $\bar{f}_i \neq \bar{0}$, $i = 1, 2$, pero, $\overline{f_1 f_2} = \bar{f}_1 \bar{f}_2 = \bar{f} = \bar{0}$.

Supongamos ahora que f es un polinomio irreducible. Si $\deg r < \deg f$ $(r \neq 0)$, entonces, el m.c.d. $(r, f) = 1$ y $ur + vf = 1$ para algunos $u, v \in P[X]$ (véase el teorema 3 del § 3 del cap. 5). En otras palabras,

$$\{r + (f)\}\,\{u + (f)\} = ru + (f) = 1 - vf + (f) = 1 + (f),$$

de donde

$$\bar{r}\bar{u} = \overline{ru} = \bar{1}.$$

Por consiguiente, cualquier elemento $\bar r \neq \bar 0$ tiene en $P[X]/(f)$ su recíproca $\bar u = \bar r^{-1}$. Esta observación muestra que, en el caso de un polinomio f irreducible, el anillo cociente $P[X]/(f)$ es un campo, contenedor de un subcampo isomorfo a P.

Prestemos atención al elemento especial $\bar X \in P[X]/(f)$. Para cualesquiera $a_0, a_1, \ldots, a_m \in P$ tenemos

$$\sum_{k=0}^{m} \bar a_k \bar X^k = \sum_k \{a_k + (f)\}\{X + (f)\}^k =$$

$$= \sum_k \{a_k + (f)\}\{X^k + (f)\} = \{\sum_k a_k X^k\} + (f) = \overline{\sum_k a_k X^k}.$$

En resumen, si $g(Y) = \sum a_k Y^k \in P[Y]$, entonces, $g(\bar X) = \overline{g(X)}$. La escritura $g(\bar X)$ tiene, por supuesto, sentido cuando P se identifica con el campo a él isomorfo, contenido en $P[X]/(f)$. En particular,

$$f(\bar X) = \overline{f(X)} = f + (f) = (f) = \bar 0,$$

o sea, el elemento $\bar X \in P[X]/(f)$ es raíz del polinomio (f).

Así, es legítimo el

TEOREMA 2. *El anillo de las clases de restos (anillo cociente) $P[X]/f$ resulta un campo si, y sólo si, f es un polinomio irreducible sobre P.* ■

COROLARIO. *Para cualquier polinomio irreducible $f(X)$ sobre el campo P existe una ampliación $F \supset P$ en la cual $f(X)$ tiene, por lo menos, una raíz. Como F se puede tomar un campo isomorfo a $P[X]/(f)$.* ■

De acuerdo con la terminología establecida, es aceptado decir que la ampliación F se obtuvo adjuntando a P una raíz c del polinomio f: $F = P(c)$. Con esto, $f(X) = (X - c)\, g(X)$, donde $g \in F[X]$. Se nos ha presentado la posibilidad real de construir la ampliación del campo P, en el cual el polinomio f se descompone totalmente en factores lineales.

DEFINICIÓN. Sean, P un campo y f un polinomio unitario (no necesariamente irreducible) de grado n de $P[X]$. Entonces, la ampliación $F \supset P$ se llama *campo de descomposición de f* sobre P, si $f(X) = (X - c_1) \ldots (X - c_n)$ en $f[X]$ y $F = P(c_1, \ldots, c_n)$, o sea, F se obtiene de P con la adjunción de las raíces $c_1, \ldots, c_n$ del polinomio f.

TEOREMA 3. *Para todo polinomio unitario $f \in P[X]$ de grado $n > 0$ existe por lo menos un campo de descomposición.*

DEMOSTRACIÓN. La condición de unitariedad no es esencial y se usa sólo para comodidad. Sea

$$f(X) = f_1(X) \ldots f_r(X)$$

una descomposición de f en factores unitarios irreducibles en $P(X)$. De acuerdo con el corolario del teorema 2, existe una ampliación $P_1 \supset P$, en la cual se tiene por lo menos una raíz del polinomio f_1.

Esta raíz c_1 será, por supuesto, también raíz de f. Sea que se halló la ampliación $P_k \supset \ldots \supset P_1 \supset P$, sobre la cual f tiene la descomposición

$$f(X) = (X - c_1) \ldots (X - c_k)\, g_1(X) \ldots g_s(X)$$

con k (no necesariamente distintos) factores lineales, $k < n$. Utilizando de nuevo el corolario del teorema 2 respecto al campo P_k y al polinomio unitario irreducible $g_1 \in P_k[X]$, construimos el campo $P_{k+1} \supset P_k$, que permite desprender el factor lineal $X - c_{k+1}$ con $c_{k+1} \in P_{k+1}$ del polinomio $g_1(X)$, y, en consecuencia, también del polinomio $f(X)$. Si continuamos operando de un modo semejante, llegamos a la descomposición total del polinomio f en sus factores lineales sobre alguna ampliación $P_n \supset P$. Bien P_n, bien algún subcambio suyo F, será precisamente el campo de descomposición para f. No se excluye, que F coincida con P. ∎

La demostración del teorema 3 contiene demasiada arbitrariedad, como para hablar de la unicidad del campo de descomposición de polinomio f; y, aunque de hecho el campo de descomposición, con exactitud hasta el isomorfismo, está definido unívocamente, demostrar esto es bastante difícil. No nos es necesaria, por el momento, esta propiedad complementaria del campo de descomposición.

EJEMPLOS. 1) El campo cuadrático $\mathbb{Q}(\sqrt{d})$, es el campo de descomposición del polinomio $X^2 - d$.

2) Si se agrega a Z_2 la raíz θ del polinomio irreducible $X^2 + X + 1$, entonces, se obtiene el campo $Z_2(\theta) = \{0, 1, \theta, 1 + \theta\}$ de cuatro elementos, isomorfo, tanto al campo $Z_2[X]/(X^2 + X + 1)$, como al campo $GF(4)$ del punto 6, § 4, cap. 4. Observemos, que $X^2 + X + 1 = (X - \theta)(X - \theta^2)$, o sea, $Z_2(\theta)$, es el campo de descomposición del polinomio $X^2 + X + 1$.

3) El polinomio $X^2 + 1$ no sólo es irreducible sobre $\mathbb{R}$, cuando su campo de descomposición sea $\mathbb{C}$, sino que sobre algunos otros campos, por ejemplo, sobre Z_3. Sea $\theta^2 = -1$ (si se desea, $\theta = X + (X^2 + 1)Z_3[X]$ es un elemento del campo de las clases de restos $Z_3[X]/(X^2 + 1)$). Como $X^2 + 1 = (X - \theta)(X - \theta^3)$, entonces, $Z_3(\theta) = \{a + b\theta \mid a, b \in Z_3\}$ es el campo de descomposición para $X^2 + 1$ sobre Z_3. A propósito, $Z_3(\theta)$ es isomorfo al campo de matrices $\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix}$, $a, b \in Z_3$, del ejercicio 13, § 4 del cap. 4. He aquí, la aplicación correspondiente: $a + b\theta \to a \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} + b \begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}$. Prestemos atención al hecho, de que $Z_3(\theta)^* = \langle\lambda\rangle$, $\lambda = 1 + \theta$, $\lambda^2 = -\theta$, $\lambda^3 = 1 - \theta$, $\lambda^4 = -1$, $\lambda^5 = -1 - \theta$, $\lambda^6 = \theta$, $\lambda^7 = -1 + \theta$, $\lambda^8 = 1$, o sea, el grupo multiplicativo del campo $Z_3(\theta)$ no es solamente abeliano, sino que también cíclico.

4) De acuerdo con el criterio de Eizenshtein, el polinomio $X^3 - 2$ es irreducible sobre $\mathbb{Q}$. Como no todas sus raíces son reales, entonces, $\mathbb{Q}(\sqrt[3]{2})$ no puede ser campo de descomposición. De hecho, de campo de descomposición para $X^3 - 2$ sirve $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, donde ε es la raíz primitiva de potencia 3 de 1:

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \varepsilon\sqrt[3]{2})(X - \varepsilon^2\sqrt[3]{2}).$$

3. Demostración del teorema fundamental. Del punto anterior, solamente nos son necesarias la definición de campo de descomposición y la afirmación del teorema 3.

De acuerdo con la observación hecha inmediatamente después de la definición de campo algebraicamente cerrado, es necesario establecer la existencia de por lo menos una raíz compleja del polinomio (1). Supongamos primeramente, que todos sus coeficientes son reales, además, sin limitación de generalidad, consideraremos que $a_0 = 1$, $a_n \neq 0$. Sea

$$\deg f = 2^m n_0.$$

donde n_0 es un número entero impar. Si $m = 0$, entonces, por el lema 2, el polinomio f tiene raíz, incluso real. Aplicando la inducción en m, supondremos que el teorema ha sido demostrado para todos los polinomios con coeficientes reales, la potencia de los cuales tiene la forma $2^{m'}n_0$, con $m' \leqslant m - 1$ (para el factor impar n_0 no se establece ninguna limitación).

Examinemos el campo de descomposición F del polinomio $(X^2 + 1) \times f(X)$, existente, por el teorema 3, y contenedor de $\mathbf{C}$ en calidad de subcampo. Sea $u_1, u_2, \ldots, u_n$, las raíces del polinomio f en F. Consideremos en F los elementos

$$v_{ij} = u_i u_j + a(u_i + u_j), \quad 1 \leqslant i < j \leqslant n, \tag{2}$$

donde a es algún número real dado. Hubiese correspondido escribir $v_{ij}(a)$, pero no lo haremos, para no complicar los símbolos. El número n' de los elementos del tipo (2) es igual a

$$n' = \binom{n}{2} = \frac{n(n-1)}{2} = \frac{2^m n_0 (2^m n_0 - 1)}{2} = 2^{m-1} n'_0, \tag{3}$$

donde n'_0 es un número entero impar.

El polinomio

$$f_a(X) = \prod_{1 \leqslant i < j \leqslant n} (X - v_{ij}) = X^{n'} + b_1 X^{n'-1} + \ldots + b_{n'}$$

del anillo $F[X]$ tiene grado n', y sus raíces, por definición, son todos elementos de (2). De acuerdo con las fórmulas de Viete (12) del § 1, los coeficientes $b_1, \ldots, b_{n'}$ del polinomio $f_a(X)$ serán, con exactitud hasta el signo, funciones simétricas elementales s_k de v_{ij}. Sustituyendo en $s_k(v_{12}, v_{13}, \ldots, v_{n-1\, n})$ las expresiones de los elementos v_{ij} a través de $u_1, \ldots, u_n$, obtenemos la función $h_k(u_1, \ldots, u_n) = s_k(\ldots, u_i u_j + a(u_i + u_j), \ldots)$, $k = 1, \ldots, n'$, que también es simétrica. Efectivamente, para cualquier permutación $\pi \in S_n$ (S_n es un grupo simétrico de grado n) tenemos

$$\hat{\pi} v_{ij} = u_{\pi(i)} u_{\pi(j)} + a(u_{\pi(i)} + u_{\pi(j)}) = v_{\pi(i), \pi(j)}$$

(o $v\pi(j)\,\pi(i)$, si $\pi(i) > \pi(j)$), así que π induce la permutación π en un conjunto de elementos del tipo (2). En virtud de la simetría, $s_k(v_{12}, v_{13}, \ldots, v_{n-1,\, n})$ no varía con la permutación de los argumen-

tos, por eso

$$(\pi h_k)(u_1, \ldots, u_n) = s_k(\hat{\pi}v_{12}, \hat{\pi}v_{13}, \ldots, \hat{\pi}v_{n-1,n}) = \\ = s_k(v_{12}, v_{13}, \ldots, v_{n-1,n}) = h_k(u_1, \ldots, u_n).$$

Notemos, que $h_k(u_1, \ldots, u_n)$ es, cuando $X_i = u_i$, $i = 1, \ldots, n$, el valor del polinomio simétrico $h_k(X_1, \ldots, X_n)$ con coeficientes reales que dependen solamente de $a \in \mathbb{R}$.

Por el teorema fundamental de los polinomios simétricos (teorema 1 del § 2), existirá un polinomio $g_k(Y_1, \ldots, Y_n)$ con coeficientes reales tal, que $h_k(X_1, \ldots, X_n) = g_k(s_1(X_1, \ldots, X_n), \ldots, s_n(X_1, \ldots, X_n))$. En consecuencia,

$$(-1)^k b_k = h_k(u_1, \ldots, u_n) = g_k(s_1(u_1, \ldots, u_n), \ldots \\ \ldots, s_n(u_1, \ldots, u_n)) = g_k(-a_1, \ldots, (-1)^n a_n) \in \mathbb{R}$$

(recordemos, que a_i son los coeficientes del polinomio unitario $f \in \mathbb{R}[X]$, considerado).

Y bien, los coeficientes b_k del polinomio $f_a(X)$ resultaron reales para cualquier $a \in \mathbb{R}$. Como $\deg f_a = n' = 2^{m-1} n_0'$ (véase (3)), entonces, por presupuesto de la inducción, f_a tiene por lo menos una raíz compleja, que, por supuesto, debe coincidir con uno de los v_{ij}. Modificando el parámetro $a \in \mathbb{R}$, que se encuentra a nuestra disposición, obtendremos otros polinomios $f_a(X)$ con coeficientes reales. Pero, a cada uno de ellos, le corresponde un par de índices $i < j$ (dependiente de a) tal, que el elemento $v_{ij} = u_i u_j + a(u_i + u_j) \in F$ está contenido en el subcampo $\mathbb{C}$ del campo F. Como los distintos pares de índices $i < j$ son en total $\binom{n}{2}$, y los números reales $a \in \mathbb{R}$ son infinitamente muchos, entonces, se encontrarán dos números reales distintos a, a', con un mismo par de índices correspondientes, digamos, $i = 1$, $j = 2$ (esto es cuestión de cómo se numeran las raíces $u_1, \ldots, u_n$) para los cuales

$$u_1u_2 + a(u_1 + u_2) = c, \\ u_1u_2 + a'(u_1 + u_2) = c', \quad a \neq a', \tag{4}$$

serán números complejos. Del sistema de ecuaciones (4) se deduce, que también

$$u_1 + u_2 = \frac{c - c'}{a - a'}, \quad u_1u_2 = c - a\frac{c - c'}{a - a'}$$

pertenecen al campo $\mathbb{C}$. En tanto esto es así, los elementos u_1, u_2 serán raíces del polinomio cuadrado

$$(X - u_1)(X - u_2) = X^2 - (u_1 + u_2)X + u_1u_2$$

con coeficientes complejos. Por las fórmulas conocidas

$$u_1, u_2 = \frac{u_1 + u_2}{2} \pm \sqrt{\left(\frac{u_1 + u_2}{2}\right)^2 - u_1u_2},$$

así que u_1, u_2 también resultan ser números complejos. De este modo, para el polinomio examinado $f(X)$ con coeficientes reales, se han hallado incluso dos raíces complejas.

Sea ahora

$$f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$$

un polinomio de grado n con coeficientes complejos arbitrarios (puede considerarse $a_0 = 1$), pero esto no tiene importancia). Sustituyendo todos los a_i por los números complejos conjugados, obtenemos el polinomio

$$\bar{f}(X = \bar{a}_0X^n = \bar{a}_1X^{n-1} + \ldots + \bar{a}_{n-1}X + \bar{a}_n.$$

Introduzcamos el polinomio

$$e(X) = f(X)\bar{f}(X) = e_0X^{2n} + e_1X^{2n-1} + \ldots + e_{2n}$$

de grado $2n$ con coeficientes

$$e_k = \sum_{i+j=k} a_i\bar{a}_j, \quad k = 0, 1, \ldots, 2n.$$

Como la operación de conjugación $z \mapsto \bar{z}$ es un automorfismo de orden 2 del campo $\mathbb{C}$ (teorema 1, § 1 del cap. 5), entonces, $\bar{e}_k = \sum_{i+j=k} \bar{a}_ia_j = e_k$, y esto significa, que $e_k \in \mathbb{R}$. Por lo demostrado, el polinomio $e(X)$ con coeficientes reales tiene por lo menos una raíz compleja c:

$$f(c)\cdot\bar{f}(c) = e(c) = 0.$$

De aquí se deduce, que bien $f(c) = 0$, y el teorema queda demostrado, bien $\bar{f}(c) = 0$, o sea, $\bar{a}_0c^n + \bar{a}_1c^{n-1} + \ldots + \bar{a}_{n-1}c + \bar{a}_n = 0$. Aplicando a ambos miembros de esta igualdad el automorfismo de la conjugación compleja, obtenemos $a_0\bar{c}^n + a_1\bar{c}^{n-1} + \ldots + a_{n-1}c + a_n = 0$, o sea, $f(\bar{c}) = 0$. ∎

El cierre algebraico del campo $\mathbb{C}$ (y también el hecho de la existencia del campo de descomposición del polinomio) es cómodo usarlo en la resolución de distintos problemas.

EJEMPLO. Sea, $S_0(f)$ el conjunto de todas las raíces distintas del polinomio $f \in \mathbb{C}[X]$, y $S_1(f)$ el conjunto de todas sus «unidades»: $d \in S_1(f) \Leftrightarrow f(d) = 1$. Sean ahora f y g, dos polinomios cualesquiera de $\mathbb{C}[X]$. Es necesario mostrar, que

$$S_0(f) = S_0(g),\ S_1(f) = S_1(g) \Rightarrow f(X) = g(X).$$

Como, evidentemente, $S_0(f) \cap S_1(f) = \varnothing$, entonces, de acuerdo con los resultados del § 1, es suficente mostrar que $|S_0(f) \cup S_1(f)| \geqslant n + 1$, donde $n = \deg f$. Por el teorema 1

$$f(X) = a_0\prod_{i=1}^{\nu}(X - c_i)^{k_i},\quad f(X) - 1 = a_0\prod_{j=1}^{\mu}(X - d_j)^{l_j},\quad c_i, d_j \in \mathbb{C},$$

donde

$$\sum s_i = n = \sum t_j, \quad \nu + \mu = |S_0(f) \cup S_1(f)|.$$

De acuerdo con el teorema 5 del § 1, tenemos

$$f(X)' = (f(X) - 1)' = \prod_{i=1}^{\nu} (X - c_i)^{s_i - 1} \prod_{j=1}^{\mu} (X - d_j)^{t_j - 1} \cdot h(X),$$

de modo que $(n - \nu) + (n - \mu) = \sum (s_i - 1) + \sum (t_j - 1) \leqslant \deg f(X)' = n - 1$. En consecuencia,

$$\nu + \mu \geqslant n + 1.$$

§ 4. POLINOMIOS CON COEFICIENTES REALES

1. Descomposición en factores irreducibles en $\mathbb{R}[X]$. Del teorema 1 del § 3 se deriva que cada polinomio f de grado n en $\mathbb{C}[X]$ puede ser escrito y, además, de un modo único (con exactitud hasta la permutación de los factores) en la forma

$$f(X) = a(X - c_1)(X - c_2) \ldots (X - c_n),$$

donde $a \neq 0$, $c_1, \ldots, c_n$ son números complejos. Sea ahora $f(X) = X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$ un polinomio unitario con coeficientes reales $a_1, \ldots, a_n$ y c alguna raíz compleja del mismo: $c = u + iv$, $v \neq 0$. Aplicando a la relación $f(c) = 0$ el automorfismo de conjugación compleja, tal como hicimos en la demostración del teorema 1 del § 3, obtenemos que también $f(\bar{c}) = 0$, por cuanto $\bar{a}_i = a_i$. Por consiguiente, $f(X)$ es divisible por un polinomio de segundo grado

$$g(X) = (X - c)(X - \bar{c}) = X^2 - (c + \bar{c})X + c\bar{c} = \\ = X^2 - 2uX + (u^2 + v^2)$$

con discriminante negativo $D(g) = 4u^2 - 4(u^2 + v^2) = -4v^2 < 0$. La condición $D(g) < 0$ es necesaria y suficiente para que el polinomio cuadrado $g \in \mathbb{R}[X]$ sea irreducible sobre $\mathbb{R}$.

Si, luego, k es la multiplicidad de la raíz c del polinomio $f(X)$ y $l \leqslant k$ es la multiplicidad de la raíz $\bar{c}$, entonces, $f(X)$ se divide por el polinomio de l-ésimo grado $g(X)$:

$$f(X) = g(X)^l q(X).$$

El cociente $q(X)$ de dos polinomios de $\mathbb{R}[X]$ también será polinomio de $R[X]$, además, para $k > l$ el elemento $c \in \mathbb{C}$ será su raíz de multiplicidad $k - l$, mientras que $\bar{c}$ no es raíz. Vimos, sin embargo, que esto no es así. Por lo tanto, $k = l$ (la suposición $l \geqslant k$ se examina análogamente), o sea, las raíces complejas de cualquier polinomio de $R[X]$ son conjugadas de dos en dos. Llegamos a la conclusión de que para los elementos del anillo factorial $\mathbb{R}[X]$ es legítima la siguiente afirmación.

TEOREMA 1 *Cualquier polinomio unitario $f \in \mathbb{R}[X]$ de grado n se descompone de un modo único (con exactitud hasta el orden de los factores) en el producto de $m \leqslant n$ polinomios lineales $X - c_i$, que corresponden a sus raíces reales $c_1, \ldots, c_m$, y de $(n - m)/2$ polinomios cuadrados, irreducibles sobre $\mathbb{R}$ y correspondientes a los pares de raíces complejas conjugadas.* ∎

OBSERVACIONES. 1) Un polinomio irreducible de $\mathbb{R}[X]$ bien es lineal, bien es cuadrático, con discriminante negativo.

2) En las designaciones del teorema 1 tiene lugar la relación

$$D(f) = (-1)^{\frac{n-m}{2}} |D(f)|,$$

o sea, el signo del discriminante queda determinado por el número de pares de raíces complejas conjugadas. Esta relación puede obtenerse directamente de la definición de discriminante, o bien con ayuda de la fórmula contenida en el ejercicio 5 del § 2.

3) Las fracciones racionales elementales en el campo $\mathbb{R}(X)$ tienen la forma (9) del § 4, cap. 5.

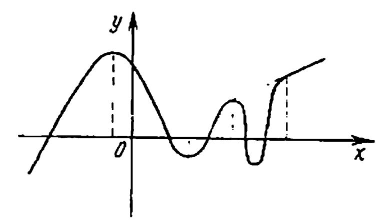
2. Problema de localización de las raíces de un polinomio. Examinaremos el polinomio $f \in \mathbb{R}[X]$ como una función de valores reales $x \to f(x)$ del argumento real x, representando la última con una gráfica en el plano con el sistema de coordenadas cartesianas xOy. A las raíces reales del polinomio $f(x)$ (o a los ceros de la función $f(x)$) responden las abscisas de los puntos de intersección de la gráfica con el eje de las x.

La primer cuestión importante, con la que habitualmente se tropieza en la práctica, se refiere a los límites de las raíces reales, o sea, al intervalo $a < x < b$, dentro del cual deben estar todas las raíces reales del polinomio f dado. Hablando con propiedad, del lema 1 del § 3 ya sabemos, que para $|x| > \frac{A}{|a_0|} + 1$ (a_0 es el coeficiente superior, $A = \text{máx}\{|a_1|, \ldots, |a_n|\}$) la función $f(x)$ no se reduce a cero, incluso si pasáramos al plano complejo. En los ejercicios 1—4 se indican límites más exactos para las raíces.

El problema más general de *localización* (*separación*) *de las raíces* de un polinomio consiste en indicar para cada una de las raíces reales el intervalo dentro del cual se encuentra solamente una raíz real. La primera resolución satisfactoria de este problema, aunque un poco voluminosa, fue obtenida por Sturm en 1829. Nos limitaremos a la demostración de resultados más parciales, teniendo en cuenta, que la resolución total del problema de localización de las raíces (especialmente si se consideran todas las raíces, incluyendo las complejas, cuando no se habla de intervalos sino que de dominios sobre el plano complejo $\mathbb{C}$) se obtiene a un precio muy alto, y su simplificación para unas u otras clases especiales de polinomios, es objeto de particular preocupación de los especialistas. No nos

referiremos en absoluto acerca de los métodos de cálculo de la «raíz localizada» con un grado de exactitud dado. La moderna matemática de computación dispone de un amplio arsenal de medios para este fin. Entrar en detalles aquí, sería inoportuno.

Felizmente, en muchos casos puede ser suficiente un cuadro cualitativo aproximado de la ubicación de las raíces. Una información fundamental brinda la construcción de la gráfica de la función $x \to f(x)$, cuyos valores fueron calculados (por ejemplo, con ayuda del esquema de Horner) aunque más no sea para los puntos donde el argumento x toma valores enteros.



Cabe esperar que las raíces de la ecuación algebraica $f(x) = 0$ se hallen entre los puntos extremos (o en los puntos extremos), que son a su vez raíces de la ecuación algebraica $f'(x) = 0$ de grado inferior. El examen de la gráfica permite, en todo caso, obtener evaluaciones por debajo para el número de raíces positivas y negativas, precisamente evaluaciones y no valores exactos, por cuanto, hablando en general, las oscilaciones de la función $x \to f(x)$ en algunos intervalos angostos pudieron ser no tomadas en cuenta por nosotros. Es notable la circunstancia, de que las evaluaciones por encima para estas mismas magnitudes se obtienen de razonamientos muy sencillos, señalados por Descartes ya en 1637. Introduzcamos la siguiente

DEFINICION. Sean

$$a_0, a_{i_1}, a_{i_2}, \ldots, a_{i_q} \quad (0 < i_1 < i_2 < \ldots < i_q \leqslant n) \qquad (1)$$

todos los coeficientes no nulos del polinomio $f(X) = a_0X^n + a_1X^{n-1} + \ldots \in \mathbb{R}[X]$, escrito en un orden dado. Si $a_{i_k}a_{i_{k+1}} < 0$, entonces, se dice, que en el $(k+1)$-ésimo término tiene lugar un *cambio de signo*. El número total de los cambios de signos en la sucesión (1) se designa con el símbolo $L(f)$.

Es claro, que siempre $0 \leqslant L(f) \leqslant \deg f$, además, $L(-f) = L(f)$. Notemos también, que $L(f) = L(aX^k + a_{i_1}X^{n-i_1} + \ldots)$, donde el exponente k satisface la única condición $k > n - i_1$, y $aa_0 > 0$. Si $L(f) = 0$, entonces, evidentemente, f no tiene raíces positivas. Por otro lado, f puede no tener raíces positivas aún en el caso en que $L(f) = \deg f$. Ejemplo: $f(X) = X^2 - X + 1$. De todos modos,

como veremos, el símbolo $L(f)$ tiene relación directa con el número de raíces positivas del polinomio f.

LEMA. *Si $c > 0$, entonces, $L((X-c)f) = L(f) + 1 + 2s$, donde $s \in \mathbf{Z}$, $s \geqslant 0$.*

DEMOSTRACIÓN. Se supone, claro está, que $f \neq 0$, así que el símbolo $L(f)$ tiene sentido. Si $\deg f = 0$, entonces, $L(f) = 0$, y el lema es válido con $s = 0$. Razonando por inducción con respecto a $\deg f$, supongamos que el lema está demostrado para todos los polinomios de grado $< n$. Sea, $\deg f = n$ y

$$f = a_0X^n + a_kX^{n-k} + \ldots + a_{n-1}X + a_n,$$

donde a_k es el primer coeficiente, después de a_0, distinto de cero, si es que tal existe ($k \geqslant 1$). Como $L(-f) = L(f)$, entonces, sin limitación de generalidad, consideramos que $a_0 > 0$. Hagamos

$$g(X) = a_kX^{n-k} + \ldots + a_{n-1}X + a_n.$$

Es claro, que

$$L(f) = L(g) + \varepsilon, \qquad (2)$$

donde

$$\varepsilon = \frac{1}{2}\left(1 - \frac{a_0a_k}{|a_0a_k|}\right) = 0 \text{ ó } 1.$$

Nuevamente se supone que $g \neq 0$, de lo contrario, la demostración para f es evidente. Hagamos también, para lo sucesivo,

$$(X-c)\,g(X) = a_kX^{n+1-k} + h(X)$$

(observemos que $g \neq 0 \Rightarrow h \neq 0$).

Por presupuesto de la inducción, en virtud de la igualdad (2)

$$L((X-c)\,g(X)) = L(g) + 1 + 2t = L(f) + 1 - \varepsilon + 2t. \qquad (3)$$

También tenemos

$$(X-c)\,f = a_0X^n(X-c) + (X-c)\,g = a_0X^{n+1} - a_0cX^n + a_kX^{n+1-k} + h(X).$$

Si $k > 1$, entonces, evidentemente, $L((X-c)f) = 2 - \varepsilon + L((X-c)g)$, por cuanto $c > 0$ ($2 - \varepsilon$ es el número de cambios de signos en la sucesión a_0, $-a_0c$, a_k). Tomando en cuenta (3) obtenemos

$$L((X-c)f) = L(f) + 1 + 2s, \quad \text{donde} \quad s = t + 1 - \varepsilon \geqslant 0.$$

Falta examinar el caso cuando $k = 1$:

$$(X-c)\,f = a_0X^{n+1} + (a_1 - a_0c)\,X^n + h(X).$$

Si a_1 y $a_1 - a_0c$ tienen igual signo, entonces,

$$L((a_1 - a_0c)\,X^n + h(X)) = L((X-c)\,g)$$

y

$$L((X-c)f) + \varepsilon + L((X-c)g) = L(f) + 1 + 2s, \quad s = t.$$

Si a_1 y $a_1 - a_0c$ tienen signo contrario, lo que es posible sólo cuando $a_0 > 0$ y $\varepsilon = 0$, entonces,

$$L((a_1 - a_0 - a_0c)X^n + h(X)) = L((X-c)g) \pm 1 = \\ = L(f) + 1 + 2t \pm 1$$

y

$$L((X-c)f) = 1 + L((a_1 - a_0c)X^n + h(X)) = L(f) + 1 + 2s,$$

donde $s = t$ ó $t + 1$. Finalmente, si $a_1 - a_0c = 0$, lo que, nuevamente, es posible solamente cuando $a_0 > 0$ y $\varepsilon = 0$, entonces,

$$L((X-c)f) = L(a_0X^{n+1} + h(X)) = L(a_1X^n + h(X)) = \\ = L((X-c)g) = L(f) + 1 + 2s, \quad s = t. \quad ■$$

Con ayuda del lema demostrado se obtiene fácilmente la *regla de los signos de Descartes.*

TEOREMA 2. *El número de raíces positivas del polinomio f con coeficientes reales coincide con $L(f)$ o es menor en un número par.*

DEMOSTRACIÓN. Sean $c_1, c_2, \ldots, c_m$, las raíces positivas (no necesariamente distintas) del polinomio $f(X) = a_0X^n + \ldots \ldots + a_{n-\nu}X^\nu$, donde, por condición, $a_0 > 0$ y $a_{n-\nu}$ es el último coeficiente distinto de cero. Recordando la forma canónica de descomposición de un polinomio (teorema 1), podemos escribir:

$$f(X) = (X - c_1) \ldots (X - c_m)\, g(X), \tag{4}$$

donde $g(X) = a_0X^{n-m} + \ldots + bX^\nu$, $a_0 > 0$, $b > 0$ $(\nu \geqslant 0)$. Como a_0 y b son de igual signo, entonces, $L(g) = 2t$ es un número par. Tomando en cuenta el lema y la descomposición (4), se obtiene la cadena de igualdades

$$L((X-c_1)g) = 1 + 2(s_1 + t),$$
$$L((X-c_2)(X-c_1)g) = 1 + 2(s_1 - t) + 1 + 2s_2 = 2 + 2(s_1 + s_2 + t),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$L(f) = m + 2(s_1 + s_2 + \ldots + s_m + t).$$

La última de ellas precisamente expresa la afirmación del teorema. ■

Y bien, siempre $m \leqslant L(f)$. Nos detendremos ahora en el importante caso práctico, cuando, por alguna razón, sabemos de antemano que todas las raíces del polinomio f son reales. Entonces tiene lugar la especificación del teorema de Descartes.

TEOREMA 3. *Si todas las raíces del polinomio f son reales, entonces, para un número $m(f) = m$ de sus raíces positivas, teniendo en cuenta las multiplicidades, es legítima la igualdad $m(f) = L(f)$.*

DEMOSTRACIÓN. Hubiese sido relativamente fácil deducir el teorema 3 del 2, pero es igualmente sencilla (y, además, instructiva) la demostración independiente en la que nos detendremos.

Por el conocido teorema de Rolle del análisis (o del teorema del valor medio), entre las raíces a' y b' de nuestro polinomio $f(X)$, existe un número $c \in \mathbb{R}$, $a' < c < b'$, para el que $f'(c) = 0$. De aquí se deriva que todas las raíces de la derivada $f'(X)$ son reales y que $m(f') = m(f)$ o $m(f) - 1$. En efecto, sean $c_1 < c_2 < \ldots < c_r$ las raíces del polinomio f de multiplicidades $n_1, n_2, \ldots, n_r$ tales que $n_1 + n_2 + \ldots + n_r = \deg f = n$. Por el teorema 5 del § 1, la derivada f' tiene las raíces $c_1, c_2, \ldots, c_r$ de multiplicidades $n_1 - 1$, $n_2 - 1, \ldots, n_r - 1$, y en los intervalos entre ellas, por el teorema de Rolle, por lo menos una raíz más $c'_1, c'_2, \ldots, c'_{r-1}$. En total, se obtienen $(n_1 - 1) + \ldots + (n_r - 1) + r - 1 = n - 1$ raíces reales. Como $\deg f' = n - 1$, entonces, f' no tiene otras raíces. Sean, luego, $c_{l-1} < 0$, y $c_l, \ldots, c_r$ todas las raíces positivas de multiplicidades $n_l, \ldots, n_r$: $n_l + \ldots + n_r = m = m(f)$. Las raíces $c_l, \ldots, c_r$ de multiplicidades $n_l - 1, \ldots, n_r - 1$, así como las $c'_l, \ldots, c'_r$ y, posiblemente, también la raíz c'_{l-1}, serán las raíces positivas de la derivada $f'(X)$, o sea, el número de ellas será $m(f') = m(f) - 1$ o $m(f)$, como se afirmó. Sirve de expresión analítica de este hecho, la casi tautológica fórmula

$$m(f = m(f') + \varepsilon, \quad \varepsilon = \frac{1}{2}(1 - (-1)^{m(f)+m(f')}). \tag{5}$$

Observemos también, que si

$$f(X) = a_0X^n + \ldots + a_{n-\nu}X^{\nu}, \tag{6}$$

donde $a_{n-\nu}$ es el último coeficiente distinto de cero, entonces, en correspondencia con la escritura de (4), $a_{n-\nu} = (-1)^m c_{l_1}c_{l_2} \ldots c_{l_m}b$, donde $c_{l_k} > 0$ y $b > 0$. En otras palabras,

$$(-1)^{m(f)} a_{n-\nu} > 0. \tag{7}$$

Razonando ahora por inducción con respecto a $n = \deg f$, supongamos que el teorema está demostrado para todos los polinomios de grado $< n$. Si en (6) $\nu > 0$, o sea, $a_n = 0$, entonces, $f(X) = X \cdot f_1(X)$ además, $m(f) = m(f_1) = L(f_1) = L(f)$ $(m(f_1) = L(f_1)$, por inducción. Queda por examinar el caso en que $a_n \neq 0$. Sea

$$f'(X) = na_0X^{n-1} + \ldots + \mu a_{n-\mu}X^{\mu-1}, \quad a_{n-\mu} \neq 0.$$

Entonces

$$L(f) = L(f' + \delta, \quad \delta = \frac{1}{2}\left(1 - \frac{a_na_{n-\mu}}{|a_na_{n-\mu}|}\right) = 0 \text{ ó } 1.$$

Pero sabemos (véase (7)), que $(-1)^{m(f)}a_n > 0$ y $(-1)^{m(f')}a_{n-\mu} > 0$. Por eso, $\delta = \frac{1}{2}(1 - (-1)^{m(f)+m(f')})$ y, por consiguiente, $\delta = \varepsilon$.

Como, por presupuesto de la inducción, $L(f') = m(f')$, entonces, en difinitiva, tenemos $L(f) = m(f') + \varepsilon$ o, comparando con (5), $m(f) = L(f)$. ∎

COROLARIO (caso particular del teorema de Budan — Fourier). *Sea que todas las raíces del polinomio f son reales. Entonces, el número de sus raíces que se encuentran en el intervalo (a, b), es igual a $L(f_a) - L(f_b)$, donde*

$$f_a(X) = f(X + a) = \sum_{0 \leqslant k \leqslant n} \frac{f^{(k)}(a)}{k!} X^k,$$

$$f_b(X) = f(X + b) = \sum_{0 \leqslant k \leqslant n} \frac{f^{(k)}(b)}{k!} X^k$$

son desarrollos en series de Taylor (véase el ejercicio 3).

DEMOSTRACIÓN. Por definición, el número $m(f_a)$ de raíces positivas del polinomio f_a es igual al número de raíces del polinomio dado f, mayores que a. La misma observación se refiere a f_b. En consecuencia, el número de raíces del polinomio f, comprendidas entre a y b $(a < b)$, es igual a la diferencia $m(f_a) - m(f_b)$, la cual, por el teorema 2, se expresa en la forma $L(f_a) - L(f_b)$. ∎

3. Polinomios estables. El polinomio unitario

$$f(X) = X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$$

con coeficientes reales, se llama *estable*, si todas sus raíces se encuentran en el semiplano izquierdo:

$$f(\lambda) = 0, \quad \lambda = \alpha + i\beta \Rightarrow \alpha < 0$$

(véase la fig. 19). La terminología tiene su origen en la teoría de ecuaciones diferenciales. Los criterios de estabilidad asintótica del comportamiento de un

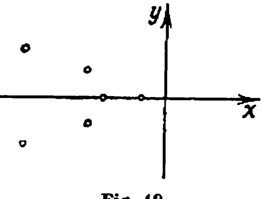


Fig. 19

sistema físico (y, en un sentido más amplio, mecánico, técnico o económico) en el entorno de la situación de equilibrio, obtenidos en esta teoría, requieren que

$$\lim_{t \to +\infty} e^{\lambda t} = 0, \tag{8}$$

donde λ es una raíz cualquiera del polinomio f, asociada a la ecuación diferencial de orden n con coeficientes constantes. Como por la fórmula de Euler (véase (15),

§ 1 del cap. 5) $e^{\lambda t} = e^{\alpha t}e^{i\beta t} = e^{\alpha t}(\cos \beta t + i \operatorname{sen} \beta t)$, entonces, el término dominante es $e^{\alpha t}$ y la condición (8) es equivalente a la desigualdad $\alpha < 0$.

Surge el problema original de localización, *el problema* de Routh—Hurwitz*), cuando directamente por los coeficientes del polinomio f, es menester aclarar si es f estable o no. Este problema algebraico fué resuelto ya en 1895. El criterio de Routh—Hurwitz dice: *el polinomio f es estable, si y sólo si, se cumplen las desigualdades*

$$\Gamma_1 > 0, \quad \Gamma_2 > 0, \ \ldots, \ \Gamma_n > 0, \tag{9}$$

donde

$$\Gamma_k = \begin{vmatrix} a_1 & 1 & 0 & 0 & 0 & 0 & \ldots & 0 \\ a_3 & a_2 & a_1 & 1 & 0 & 0 & \ldots & 0 \\ a_5 & a_4 & a_3 & a_2 & a_1 & 1 & \ldots & 0 \\ a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{2k-1} & a_{2k-2} & a_{2k-3} & a_{2k-4} & a_{2k-5} & a_{2k-6} & \ldots & a_k \end{vmatrix}$$

(se supone, que $a_s = 0$ para $s > n$).

Sin pretender demostrar el teorema de Routh—Hurwitz (esto es más propio hacerlo en otros cursos), prestamos atención a la circunstancia de que la forma elegante de su formulación se debe por completo a la teoría de los determinantes. Luego, de acuerdo con el teorema 1, cuando se cumple la condición (9) el polinomio $f(X)$ se representa en forma del producto de factores del tipo $X + u$, $X^2 + vX + w$, con $u > 0$, $v > 0$, $w > 0$ y esto significa, que todos los coefinicientes del polomio estable $f(X)$ son positivos:

$$a_1 > 0, \quad a_2 > 0, \ \ldots, \ a_n > 0. \tag{10}$$

De este modo, las condiciones (10) son necesarias para la estabilidad del polinomio $f(X)$. No siendo en el caso general suficientes, ellas permiten, sin embargo, reducir aproximadamente a la mitad el número de las desigualdades determinantes (9). Esto es cómodo, ya que el cálculo de los determinantes exige mucho trabajo.

EJEMPLO. Para $n = 2$, el sistema de desigualdades $\Gamma_1 > 0$, $\Gamma_2 > 0$, es equivalente a otro más sencillo: $a_1 > 0$, $a_2 > 0$, lo que, de paso, es evidente de las fórmulas de las raíces de la ecuación cuadrática.

Para $n = 3$ todo se reduce a las desigualdades $a_1 > 0$, $a_2 > 0$, $a_3 > 0$, $a_1a_2 > a_3$, por cuanto $\Gamma_3 = a_3(a_1a_2 - a_3)$.

Finalmente, observemos que el criterio de Routh—Hurwitz no resuelve todas las cuestiones vinculadas con la estabilidad, por cuanto, en la práctica, se trata de polinomios y de ecuaciones diferenciales, cuyos coeficientes dependen de un parámetro. Las condiciones de estabilidad deben formularse en términos del propio parámetro, lo que ya es una tarea de naturaleza totalmente distinta.

EJERCICIOS

1. Sea $f(X) = a_0X^n + a_1x^{n-1} + \ldots + a_n$ un polinomio real de grado n. Mostrar, que el conocimiento de los límites superiores de las raíces de los polinomios $f(X)$, $X^n f\left(\frac{1}{X}\right)$, $f(-X)$, $X^n f\left(-\frac{1}{X}\right)$ brinda los límites inferiores y superiores, de las raíces positivas y negativas del polinomio $f(X)$.

---

*) De hecho, formulado mucho antes (en 1868) por el físico inglés J. C. Maxwell y resuelto, para grados pequeños por el ingeniero ruso I. A. Vishnegradsky, quien se ocupaba del problema de la estabilidad de los reguladores (1876).

17—0392

2. En las designaciones del ejercicio 1 sean, $a_0 > 0$; m, el menor índice para el cual $a_m < 0$; B, el máximo de los valores absolutos de los coeficientes negativos. Mostrar, que

$$c \leqslant 1 + \sqrt[m]{B/a_0}$$

para cada raíz real positiva del polinomio $f(X)$. (*Indicación*. Para $x > 1$ partir de la estimación

$$f(x) \geqslant a_0 x^n - B\frac{x^{n-m+1}-1}{x-1} > \frac{x^{n-m+1}}{x-1}[a_0 x^{m-1}(x-1) - B].)$$

3. (*Fórmula de Taylor*). Sea P un campo de característica nula, $a \in P$. Para cualquier polinomio $f \in P[X]$ de grado n, tiene lugar la fórmula

$$f(X) = f(a) + \frac{f'(a)}{1!}(X-a) + \frac{f''(a)}{2!}(X-a)^2 + \ldots + \frac{f^{(n)}(a)}{n!}(X-a)^n.$$

(*Indicación*. Derivar k veces la expresión formal

$$f(X) = \sum b_i (X-a)^i \text{ y hacer } X = a.)$$

4. Mostrar, que si $f(a) > 0$, $f'(a) > 0$, . . ., $f^{(n)}(a) > 0$ para el polinomio real $f(X)$ de grado n y con coeficiente superior a_0 positivo, entonces, $f(c) = 0$, $c > 0 \Longrightarrow c < a$. (*Indicación*. Aplicar el ejercicio 3.)

5. Aprovechando la regla de los signos de Descartes, hallar el signo del discriminante de los polinomios $X^5 - X^2 + 1$, $X^3 - 6X - 9$ (véase la observación al final del punto 1).

6. ¿Pueden los polinomios $X^5 - X - 1$ y $X^3 + aX + b \in \mathbb{Q}[X]$ tener raíces complejas comunes? Recordemos (véase el cj. 10, del § 1), que el polinomio $X^5 - X - 1$ es irreducible sobre $\mathbb{Q}$.

7. Mostrar, que las raíces del polinomio $f(X) = X^5 + uX^4 + vX^3 + w \in \mathbb{R}[X]$ con término independiente $w \neq 0$, no pueden ser todas reales. (*Indicación*. Es cómodo pasar *al polinomio recíproco* $X^5 f\left(\frac{1}{X}\right)$ y luego utilizar las fórmulas (12) del § 1, y (9) del § 2.)

8. Es claro, que si el polinomio entero $f(X) = a_0X^n + \ldots + a_n$ tiene una raíz $c \in \mathbb{Z}$, entonces, c divide el término independiente $a_n = f(0)$: $f(c) = 0 \Rightarrow a_n = c(-a_0c^{n-1} - \ldots - a_{n-2}c - a_{n-1})$. Mostrar que, a un mismo tiempo, $c - 1$ divide $f(1) = \sum a_i$ y $c + 1$ divide $f(-1) = \sum(-1)^i a_i$. (*Indicación*. $f(X) = (X - c)\, g(X) \Rightarrow g(X) \in \mathbb{Z}[X]$.) Aplicar estos razonamientos a la búsqueda de las raíces enteras del polinomio $X^4 + X^3 - X^2 + 40X - 100$ (*respuesta*: $c = 2$).

9. Convencerse, de que

$$f(X) = X^n + a_1X^{n-1} + \ldots + a_n \in \mathbb{Z}[X], \quad f(c) = 0, \quad c \in \mathbb{Q} \Rightarrow c \in \mathbb{Z}.$$

(*Indicación*. Si $c = a/b$ es una fracción irreducible, entonces, $a^n/b = -a_1a^{n-1} - a_2a^{n-2}b - \ldots - a_nb^{n-1}$). ¿Qué se puede decir acerca de las raíces racionales del polinomio entero con coeficiente superior $a_0 \neq 1$?

10. Cualquier polinomio $f(X)$ con $f(x) \geqslant 0$ para todas las $x \in \mathbb{R}$ se puede representar en la forma

$$f(X) = g(X)^2 + h(X)^2,$$

donde $g, h \in \mathbb{R}[X]$. (*Indicación*. Con ayuda del teorema 1 descomponer $f(X)$ en factores del tipo $(X + a)^2 + b^2$, y aprovechar la identidad formal

$$(p^2 + q^2)(r^2 + s^2) = (pr + qs)^2 + (ps - qr)^2,$$

que se deriva de la relación

$$|p + iq|^2 |r + is|^2 = |(p + iq)(r + is)|^2).$$

11. Obtener independientemente los criterios de estabilidad de los polinomios de grados 3 y 4. Para $n = 4$ escribir el mismo en forma de las desigualdades: $a_1 > 0$, $a_4 > 0$, $a_1a_2 > a_3$, $a_3(a_1a_2 - a_3) > a_1^2a_4$. (*Indicación*. $f(X) = X^3 + aX^2 + bX + c = (X^2 + \alpha X + \beta)(X + \theta)$, donde $a = \alpha + \theta$, $b = \beta + \alpha\theta$, $c = \beta\theta$, además, α, β, $\theta \in \mathbb{R}$. La estabilidad de $f(X)$ es equivalente a la estabilidad de los pares de polinomios $X^2 + \alpha X + \beta$, $X + \theta$, o sea, al cumplimiento de las desigualdades $\alpha > 0$, $\beta > 0$, $\theta > 0$. Se comprueba facilmente, que este sistema es equivalente al sistema de desigualdades $a > 0$ $b > 0$, $c > 0$, $ab - c > 0$. Emplear razonamientos análogos con respecto al polinomio real de cuarto grado).

«Ultimamente, cada vez es más difundido el punto de vista, que muchas de las partes de las matemáticas no son otra cosa que la teoría de invariantes de grupos especiales»

(Sofus Lie, 1893)

Parte II

GRUPOS. ANILLOS. MODULOS

El contenido de la segunda parte se puede calificar como una continuación sumamente seria pero, es de esperar, no demasiado abstracta, de la primera. Se introducen relativamente pocos nuevos conceptos. El lector encontrará sus viejos conocidos del capítulo 4, quienes lo conducirán a un dominio de ideas con mayor contenido. Se recomienda prestar máxima atención al estudio de los ejemplos, a los que se dedica casi la cuarta parte del texto (digamos, el material del § 1, cap. 7, y del § 3 cap. 8, se consideran, naturalmente, como ejemplos). Por otra parte, éstos se han seleccionado con la intención de tender un puente entre el álgebra y otras partes de las matemáticas. Si, como resultado, al lector se le fortalece el sentimiento de unidad de las matemáticas, entonces, la meta buscada por el autor en la segunda parte del libro, deberá considerarse alcanzada.

ITERATURA COMPLEMENTARIA

1. Atiyan M. Mc Donald J., Introduction to conmutative Algebra, N. Y., 1969.
2. Bartoo T., Birkhoff G., Modern Applied Algebra, N.Y., 1970.
3. V. A. Bielonógov, A. N. Fomín, Las representaciones matriciales en la teoría de los grupos finitos, «Nauka», 1976 (en ruso).
4. S. I. Boriévich, I. R. Shafarévich, Teoría de los números, «Nauka», 1972 (en ruso).
5. Bourbaki N., Algebra (módulos, anillos, formas), Ed. Univ. Nac. Santiago de Chile, 1972.
6. Cohn P., Universal Algebra, N. Y., 1965.
7. Dieudonné J., Munford D., Carrol J., Geometric Invariant Theory, W. Berlin, 1965.
8. Faith H., Algebra rings, modulos and catogories, Haidelberg, 1973.
9. Horstein I., Nonconmutativo Rings, N. Y., 1960.
10. Hall M., The Theory of Groupe, N. Y., 1950.
11. Jacobson N., Lie Algebras, N. Y., 1962.
12. L. A. Kaluzhnin, Introducción al álgebra general, «Nauka», 1973 (en ruso).
13. M. I. Kargapólov, Y. I. Merzliakov, Fundamentos de la Teoría de los grupos, «Nauka», 1972 (en ruso).
14. A. A. Kirílov, Elementos de la teoría de representaciones, «Nauka», 1972 (en ruso).
15. A. G. Kurosch, Curso de álgebra superior, Mir, 1977.

16. G. Ya. Liubarski, Teoría de los grupos y sus aplicaciones en la física, «Fismatguiz», 1958 (en ruso).
17. A. Máltsev, Sistemas algebráicos, «Nauka», 1970 (en ruso).
18. M. A. Naymark, Teoría de las representaciones de grupos, «Nauka», 1970 (en ruso).
19. L. S. Pontriaguin, Grupos contínuos, Mir, 1978.
20. M. M. Póstnikov, Teoría de Galois, «Fismatguiz», 1963 (en ruso).
21. Serre J. P., Représentations lineaires des groupes finis, Paris, 1967.
22. Serre J. P., Cours d'arithmétique, Paris, 1970.
23. Weil H., The classical Groups, Their Invariants and Representaions, Princeton, 1940.
24. D. P. Zhelobenko, Grupos compactos de Lie y sus Representationes, «Nauka», 1970 (en ruso).

Capítulo 7

GRUPOS

En este capítulo se desarrolla el concepto de grupo, introducido en el capítulo 4. En primer lugar, se hace incapié en el estudio de un género distinto de «operaciones» naturales de los grupos, y no en la consideración de grupos abstractos, a los cuales se les han dedicado muchos trabajos especiales. Precisamente, las realizaciones concretas de grupos han dado impulso al desarrollo de la teoría general de los grupos y le otorgaron a ella reputación de instrumento útil de investigación matemática.

En el fondo de ejemplos particulares (pero, observemos, importantes) se hace más insistente la idea de considerar los (homo-, epi-, iso-) morfismos de grupos, así como las estructuras teóricas de grupos, que permiten reducir el estudio de objetos complejos al de más sencillos.

§ 1. GRUPOS CLASICOS DE PEQUEÑAS DIMENSIONES

1. Definiciones generales. El curso de álgebra lineal y de geometría nos suministra nuevos tipos de grupos, merecedores de que nos detengamos en ellos con un poco de mayor atención. La separación, en los grupos de transformaciones de los subgrupos de espacios afines, euclídeos y hermitianos, que dejan en su lugar un punto fijo (por ejemplo, el origen de las coordenadas) lleva a los denominados *grupos clásicos* GL (n), SL (n), O (n), SO (n), U (n), SU (n). Observemos, que el lugar verdadero de los mismos, se halla entre los llamados grupos de Lie. Correspondería agregar por lo menos también el grupo simplicial Sp (n), pero no nos hemos propuesto la descripción de todos los grupos clásicos; esto se hace en otros libros. Para n no grandes se dicen grupos clásicos de pequeñas dimensiones. Con los grupos GL (n), SL (n), hemos tenido la oportunidad de encontrarnos antes (véase la parte I). Deseando evitar una gran dependencia de la geometría, recordemos, que la elección de la base ortonormalizada en el espacio conduce a una definición matricial equivalente de los grupos ortogonal y unitario:

$$\begin{aligned} \mathrm{O}(n) &= \{A \in M_n(\mathbb{R}) \mid {}^tA\cdot A = A\cdot{}^tA = E\},\\ \mathrm{SO}(n) &= \{A \in \mathrm{O}(n) \mid \det A = 1\},\\ \mathrm{U}(n) &= \{A \in M_n(\mathbb{C}) \mid A^*\cdot A = A\cdot A^* = E\},\\ \mathrm{SU}(n) &= \{A \in \mathrm{U}(n) \mid \det A = 1\}. \end{aligned}$$

Aquí $A^* = {}^t\bar{A}$ es la matriz que se obtiene de $A = (a_{ij})$ por transposición y sustitución de los coeficientes a_{ij} por los números com-

plejos conjugados $\bar{a}_{ij}$. Los grupos SL (n), SO (n), SU (n), llevan el nombre de *especiales* (*lineales, ortogonales* y *unitarios*). En particular,

$$O(1)=\{\pm 1\},\quad SO(1)=\{1\},$$
$$U(1)=e^{i\varphi}|0\leqslant\varphi<2\pi\},\quad SU(1)=\{1\},$$
$$SO(2)=\left\{\begin{Vmatrix}\cos\varphi & -\operatorname{sen}\varphi\\ \operatorname{sen}\varphi & \cos\varphi\end{Vmatrix}\middle|\, 0\leqslant\varphi<2\pi\right\}\cong U(1.$$

El isomorfismo entre los grupos SO (2) y U (1) se da por medio de la correspondencia natural

$$\begin{Vmatrix}\cos\varphi & -\operatorname{sen}\varphi\\ \operatorname{sen}\varphi & \cos\varphi\end{Vmatrix}\mapsto e^{i\varphi}.$$

Como la representación geométrica de los números complejos $e^{i\varphi}$, $0\leqslant\varphi<2\pi$ es la circunferencia S^1 de radio unitario en $\mathbb{R}^2$, entonces, se dice también, que el grupo SO (2) y la circunferencia S^1 son topológicamente equivalentes. El sentido exacto de esta terminología se explica en el curso de geometría.

Una relación admirable y mucho menos evidente existe entre los grupos SU (2) y SO (3). Detengámonos previamente en la representación geométrica del grupo SU (2), que nos llevará posteriormente a la representación geométrica del grupo SO (3).

2. Parametrización de los grupos SU (2), SO (3). Por el conocido teorema de Euler, cada elemento del grupo SO (3) de las rotaciones propias del espacio euclídeo tridimensional $\mathbb{R}^3$ es la rotación alrededor de cierto eje fijo. Digamos, las matrices

$$B_\varphi=\begin{Vmatrix}\cos\varphi & -\operatorname{sen}\varphi & 0\\ \operatorname{sen}\varphi & \cos\varphi & 0\\ 0 & 0 & 1\end{Vmatrix},\quad C_\theta=\begin{Vmatrix}1 & 0 & 0\\ 0 & \cos\theta & -\operatorname{sen}\theta\\ 0 & \operatorname{sen}\theta & \cos\theta\end{Vmatrix}\tag{1}$$

responden a las rotaciones alrededor de los ejes Oz y Ox respectivamente a los ángulos φ y θ. Utilizando la parametrización de las rotaciones con los ángulos de Euler φ, θ, ψ ($0\leqslant\varphi,\psi<2\pi$, $0\leqslant\theta<$ $<\pi$), cuyo sentido geométrico por ahora no nos interesa, cualquier matriz $A\in$ SO (3) puede escribirse en la forma,

$$A=B_\varphi C_\theta B_\psi,\tag{2}$$

donde B_φ, B_θ, B_ψ, son las matrices indicadas más arriba (1).

Sea, además,

$$g=\begin{Vmatrix}\alpha & \beta\\ \gamma & \delta\end{Vmatrix}\in SU(2).$$

Tenemos

$$g^* = {}^t\bar{g} = \begin{Vmatrix} \bar{\alpha} & \bar{\gamma} \\ \bar{\beta} & \bar{\delta} \end{Vmatrix}, \quad g^{-1} = \begin{Vmatrix} \delta & -\beta \\ -\gamma & \alpha \end{Vmatrix}.$$

Como $g \in U(2) \Leftrightarrow g^* = g^{-1}$, entonces, $\delta = \bar{\alpha}$ y $\gamma = -\bar{\beta}$. De esto modo, cualquier matriz g de SU (2) tiene la forma

$$g = \begin{Vmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{Vmatrix}, \quad |\alpha|^2 + |\beta|^2 = 1. \tag{3}$$

Inversamento, si g es una matriz del tipo (3), entonces, evidentemente, $g \in$ SU (2) En consecuencia, cada elemento del grupo SU (2) gueda determinado unívocamente por un par de números complejos α, β, tales, que $|\alpha|^2 + |\beta|^2 = 1$. Si se hacen $\alpha = \alpha_1 + i\alpha_2$, $\beta + \beta_1 + i\beta_2$ con $\alpha_k, \beta_k \in \mathbb{R}$, $i = \sqrt{-1}$, entonces, la condición $|\alpha|^2 + |\beta|^2 = 1$ escrita en forma

$$\alpha_1^2 + \alpha_2^2 + \beta_1^2 + \beta_2^2 = 1,$$

permite decir, que *el grupo* SU (2) *es topológicamente equivalente (homeomorfo) a la esfera* S^3 *en el espacio real cuatridimensional* $\mathbb{R}^4$.

Prestemos atención a las matrices unitarias

$$b_\varphi = \begin{Vmatrix} e^{i\frac{\varphi}{2}} & 0 \\ 0 & e^{-i\frac{\varphi}{2}} \end{Vmatrix}, \quad c_\theta = \begin{Vmatrix} \cos\frac{\theta}{2} & i \operatorname{sen}\frac{\theta}{2} \\ i \operatorname{sen}\frac{\theta}{2} & \cos\frac{\theta}{2} \end{Vmatrix}. \tag{4}$$

Como se demuestra en el curso de álgebra lineal (y, en el caso dado, se comprueba inmediatamente), para una matriz unitaria del tipo (3) existe una matriz unitaria u tal, que

$$g = u b_\varphi u^{-1} \tag{5}$$

con $\lambda = e^{i\frac{\varphi}{2}}$, determinado por la ecuación cuadrática

$$\lambda^2 = 2\alpha_1\lambda + 1 = 0.$$

Observemos también, que cualquier matriz (3), siendo $\alpha\beta \neq 0$, puede tomar la forma

$$a(\varphi, \theta, \psi) = b_\varphi c_\theta b_\psi = \begin{Vmatrix} \cos\frac{\theta}{2} \cdot e^{i\frac{\varphi+\psi}{2}} & i \operatorname{sen}\frac{\theta}{2} \cdot e^{i\frac{\varphi-\psi}{2}} \\ i \operatorname{sen}\frac{\theta}{2} \cdot e^{i\frac{\psi-\varphi}{2}} & \cos\frac{\theta}{2} \cdot e^{-i\frac{\varphi+\psi}{2}} \end{Vmatrix}, \tag{6}$$

donde

$$0 \leqslant \varphi < 2\pi, \quad 0 \leqslant \theta < \pi, \quad -2\pi \leqslant \psi < 2\pi \text{ *)}.$$

*) Más adelante se verá, que φ, θ ψ son los mismos ángulos de Euler. A las matrices unitarias $\pm g$ se las pone en correspondencia a un mismo giro en $\mathbb{R}^3$ por eso el codominio de variación de ψ se restringe al semiintervalo $(0 \ 2\pi)$.

Es suficiente hacer

$$|\alpha|=\cos\frac{\theta}{2}, \quad \operatorname{Arg}\alpha=\frac{\varphi+\psi}{2}, \quad |\beta|=\operatorname{sen}\frac{\theta}{2}, \quad \operatorname{Arg}\beta=\frac{\varphi-\psi+\pi}{2},$$

aprovechando la circunstancia de que cada número complejo z se da mediante dos parámetros reales $|z|$ y $\arg z$ ($\operatorname{Arg} z$ es el valor principal del agrumento $\arg z$).

Ahora estamos preparados para comenzar a resolver el problema fundamental de este parágrafo.

3. Epimorfismo SU(2) → SO(3). En correspondencia a cada vector $x = x_1e_1 + x_2e_2 + x_3e_3$ del espacio euclídeo tridimensional $\mathbb{R}^3$ con norma $N(x) = x_1^2 + x_2^2 + x_3^2$, ponemos la matriz compleja de segundo orden

$$H_x=\begin{Vmatrix} x_3 & x_1+ix_2 \\ x_1-jx_2 & -x_3 \end{Vmatrix}. \tag{7}$$

El espacio M_2^+ de las matrices del tipo (7) está compuesto de todas las matrices hermíticas con traza nula (${}^t\bar{H}_x = H_x$, $\operatorname{tr} H_x = 0$), además, la correspondencia entre los vectores $x \in \mathbb{R}^3$ y las matrices $H_x \in M_2^+$ resulta, evidentemente, biunívoca. En particular, a los vectores básicos $e_1, e_2, e_3 \in \mathbb{R}^3$ les corresponden las matrices básicas $h_k = H_{e_k}$:

$$h_1=\begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}, \quad h_2=\begin{Vmatrix} 0 & i \\ -i & 0 \end{Vmatrix}, \quad h_3=\begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}; \tag{8}$$

$$H_x = x_1h_1+x_2h_2+x_3h_3,$$
$$M_2^+ = \langle h_1, h_2, h_3 \rangle_{\mathbb{R}}.$$

Observemos, que a cada operador lineal $\Phi^+\colon H_x \mapsto H_y$ en M_2^+ con matriz A en la base (8) le corresponderá un operador lineal totalmente determinado $\Phi\colon x \mapsto y$ en $\mathbb{R}^3$ con la misma matriz A en la base e_1, e_2, e_3, por cuanto $H_{\alpha x} = \alpha H_x$, $H_{x+x'} = H_x + H_{x'}$. Como en el futuro no se usarán otras bases, a veces identificaremos los operadores con las matrices que les corresponden.

Sea ahora g un elemento fijo del grupo SU (2).

Examinemos la aplicación

$$\Phi_g^+ : H_x \mapsto gH_xg^{-1}. \tag{9}$$

Como las trazas de matrices semejantes coinciden, entonces, $\operatorname{tr} \Phi_g^+(H_x) = \operatorname{tr} H_x = 0$. Además, $g^* = {}^t\bar{g} = g^{-1}$, por eso

$$(gH_xg^{-1})^* = (g^{-1})^*H_x^*g^* = gH_xg^{-1}$$

y, en consecuencia, $\Phi_g^+(H_x) \in M_2^+$:

$$\Phi_g^+(H_x)=\begin{Vmatrix} y_3 & y_1+iy_2 \\ y_1-iy_2 & -y_3 \end{Vmatrix}=H_y,$$

donde $y = (y_1, y_2, y_3) \in \mathbb{R}^3$. De las igualdades definitorias (7) y (9), se observa, que

$$\Phi_g^+ (H_{\alpha x + \alpha' x'}) = \alpha \Phi_g^+ (H_x) + \alpha' \Phi_g^+ (H_{x'}).$$

Por lo tanto, la aplicación Φ_g^+ (respectivamente, Φ_g) es el operador lineal en M_2^+ (respectivamente, en $\mathbb{R}^3$).

Mostremos, que Φ_g: $\mathbb{R}^3 \to \mathbb{R}^3$ es un operador ortogonal.

Efectivamente,

$$N(\Phi_g(x)) = N(y) = y_1^2 + y_2^2 + y_3^2 = -\det H_y = -\det \Phi_g^+(H_x) = \\ = -\det gH_xg^{-1} = -\det H_x = x_1^2 + x_2^2 + x_3^2 = N(x),$$

o sea, Φ_g conserva la norma y, en consecuencia, el producto escalar. Hasta ahora no queda claro si cambia o no Φ_g la orientación del espacio $\mathbb{R}^3$ que depende del signo del det Φ_g. Sólo sabemos que det $\Phi_g = \pm 1$.

Como se deduce de la definición,

$$\Phi_{g_1}^+ (\Phi_{g_2}^+ H_x) = g_1 (g_2 H_x g_2^{-1}) g_1^{-1} = (g_1 g_2) H_x (g_1 g_2)^{-1} = \Phi_{g_1 g_2}^+ (H_x),$$

además, Φ_E^+ es la matriz unidad ortogonal de orden 3 para $E = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} \in$ SU (2). Por lo tanto, la correspondencia

$$\Phi : g \mapsto \Phi_g \quad (0 \quad \Phi^+ : g \mapsto \Phi_g^+)$$

es un homomorfismo de SU (2) en O (3). El núcleo Ker Φ = Ker Φ^+ está formado de matrices unidades g, para las cuales $\Phi_g^+ = \Phi_E^+$. Con otras palabras

$$\text{Ker } \Phi = \{g \in \text{SU (2)} \mid gH = Hg, \forall H \in M_2^+\} = \\ = \{g \in \text{SU (2)} \mid gh_j = h_j g, \quad j = 1, 2, 3\},$$

donde h_1, h_2, h_3 son las bases (8) espacio M_2^+. La verificación directa muestra que

$$g = \begin{Vmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{Vmatrix}, \quad gh_j = h_j g, \quad 1 \leqslant j \leqslant 3 \Rightarrow g = \pm E \Rightarrow \text{Ker } \Phi = \{\pm E\}.$$

Echemos una mirada a las imágenes de las matrices unitarias (4) en presencia de un automorfismo de Φ. Efectuamos el cálculo para Φ^+ en la base (8):

$$b_\varphi h_1 b_\varphi^{-1} = (\cos \varphi)\ h_1 + (\text{sen } \varphi)\ h_2,$$
$$b_\varphi h_2 b_\varphi^{-1} = (-\text{sen } \varphi)\ h_1 + (\cos \varphi)\ h_2,$$
$$b_\varphi h_3 b_\varphi^{-1} = h_3.$$

Por lo tanto (aquí pasamos libremente de Φ^+ a Φ y de las matrices a los operadores), $\Phi_{b_\varphi} = B_\varphi$ (véase (1)) es el giro del espacio euclídeo tridimensional $\mathbb{R}^3$ en el ángulo φ alrededor del eje Ox_3 (o h_3). Si se eligen tales φ y u, que se cumpla la relación (5), entonces, por cuanto Φ es un homomorfismo, tendremos

$$\Phi_g = \Phi_u \Phi_{b_\varphi} \Phi_u^{-1} \quad \text{y} \quad \det \Phi_g = \det \Phi_u \cdot 1 \cdot (\det \Phi_u)^{-1} = 1.$$

Esto muestra que, efectivamente, Φ es un homomorfismo de SU (2) en SO (3).

De modo análogo se verifica, que $\Phi_{c_\theta} = C_\theta$ es el giro a un ángulo θ alrededor del eje Ox_1. Ahora, para cualquier matriz $A \in$ SO (3) tenemos

$$A = B_\varphi C_\theta B_\psi = \Phi_{b_\varphi}\Phi_{c_\theta}\Phi_{b_\psi} = \Phi_{b_\varphi c_\theta b_\psi} = \Phi_{a(\varphi, \theta, \psi)}.$$

En consecuencia, la imagen Im Φ contiene todo el grupo SO (3), y hemos demostrado el

TEOREMA 1. *El grupo SO (3) es la imagen homomorfa del grupo SU (2) si existe el homomorfismo* Φ: $g \Rightarrow \Phi_g$ *con núcleo* Ker $\Phi = \{\pm E\}$. *Cada giro de SO (3) responde exactamente a dos operadores unitarios g y —g de SU (2)* ■.

4. Representación geométrica del grupo SO (3). Del teorema 1, se deduce inmediatamente el

COROLARIO. *El grupo SO (3) es topológicamente equivalente (homomorfo) a espacio real proyectivo tridimensional* $\mathbb{R}(P^3)$.

Efectivamente, vimos en el punto 2 que los elementos de SU (2) se hallan en correspondencia biunívoca con los puntos de la esfera S^3 en el espacio real tetradimensional $\mathbb{R}^4$. A los operadores lineales $\pm g$ SU (2) les corresponden puntos diametralmente opuestos en S^3, que con el homomorfismo Φ se juntan (identifican). Se obtiene uno de los modelos del espacio proyectivo $\mathbb{R}(p^3)$. ■

En el curso de álgebra lineal y geometría, el espacio proyectivo $\mathbb{R}(P^n)$ se define como el conjunto de rectas del espacio $\mathbb{R}^{n+1}$ que pasan por el origen de las coordenadas O. Cada una de estas rectas interseca la esfera unitaria S^n con centro en O, exactamente en dos puntos diametralmente opuestos. Dando uno de estos puntos la recta se determina unívocamente. Esto significa, que el espacio $\mathbb{R}(P^n)$ puede ser definido como espacio cociente de la esfera unitaria S^n de $\mathbb{R}^{n+1}$, en relación a la equivalencia establecida para los puntos diametralmente opuestos de la esfera S^n. En nuestro problema no entra ahora la tarea de topología en $\mathbb{R}(P^n)$.

Hemos llegado a un resultado relativamente inesperado. En la esfera S^3 y en el espacio proyectivo $\mathbb{R}$ (P^3) se establecen estructuras de grupo: en el primer caso $SU(2)$, en el segundo $SO(3)$. Cualquier intento de dar la estructura de un grupo continuo en S^2 o en $\mathbb{R}$ (P^2) sufrirá un fracaso (resultado que no tiene vinculación con nuestro tema).

De acuerdo con el teorema 1 y su corolario, el grupo $SO(3)$ es «dos veces menor» que $SU(2)$. La existencia del epimorfismo $SU(2) \to SO(3)$ hace natural el preguntar sobre la existencia del monomorfismo $SO(3) \to SU(2)$. Veremos en el cap. 8, que la respuesta a este interrogante es negativa.

EJERCICIOS

1. Llenar las lagunas en la demostración del teorema 1, o sea, comprobar efectivamente (sin citar el curso de álgebra lineal y geometría) todas las pequeñas afirmaciones, comenzando con la igualdad (2).

2. Utilizando la representación geométrica del grupo $SU(2)$, mostrar que $(0, 1, 0, 0) * (0, 0, 1, 0) = (0, 0, 0, 1) \neq (0, 0, 1, 0) * (0, 1, 0, 0) *$ (producto de puntos en S^3). Los mismos puntos $(0, 1, 0, 0)$, $(0, 0, 1, 0)$, examinados en $\mathbb{R}$ (P^3), son permutables.

3. Mostrar, que si los coeficientes de las matrices unidades

$$K_1(t) = \begin{Vmatrix} \cos\frac{t}{2} & i\,\text{sen}\,\frac{t}{2} \\ i\,\text{sen}\,\frac{t}{2} & \cos\frac{t}{2} \end{Vmatrix}, \quad K_2(t) = \begin{Vmatrix} \cos\frac{t}{2} & -\text{sen}\,\frac{t}{2} \\ \text{sen}\,\frac{t}{2} & \cos\frac{t}{2} \end{Vmatrix},$$

$$K_3(t)=\begin{Vmatrix} e^{i\frac{t}{2}} & 0 \\ 0 & e^{-i\frac{t}{2}} \end{Vmatrix}$$

se diferencian con respecto a t haciendo luego $t = 0$, entonces, se obtienen las matrices

$$K_1=\frac{i}{2}\begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}=\frac{i}{2}h_1,\quad K_2=\frac{i}{2}\begin{Vmatrix} 0 & i \\ -i & 0 \end{Vmatrix}=\frac{i}{2}h_2,$$

$$K_3=\frac{i}{2}\begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}=\frac{i}{2}h_3,$$

que conforman la base del espacio M_2^- de *las matrices hermíticas antisimétricas*

$$K=\begin{Vmatrix} ik_3 & -k_2+ik_1 \\ k_2+ik_1 & -ik_3 \end{Vmatrix},\quad k_j\in\mathbb{R},$$

con traza nula: $K^* = -K$, $tr\ K = 0$.

§ 2. OPERACIÓN DE LOS GRUPOS EN LOS CONJUNTOS

1. Los homomorfismos G→ S(Ω). Para nosotros, la teoría de grupos comenzó en el capítulo 4 con ejemplos de grupos de transformaciones, los subgrupos del grupo $S(\Omega)$ de todas aas aplicaciones biunívocas del conjunto Ω en sí mismo. Esta forma de acceder al tema, respondo al camino histórico por el que se desarrolló esta teoría, y al significado que los grupos de transformaciones tienen en otras partes de las matemáticas. La llamada teoría abstracta de los grupos, fruto de una época posterior (primera mitad de nuestro siglo), se alejó de los grupos de transformaciones, pero muchos de sus conceptos llevan la marca de los viejos tiempos. Precisamente, la fuente de esos conceptos la hallamos en la idea de *realización* (*representación*) del grupo dado G en $S(\Omega)$, donde Ω es un conjunto elegido adecuadamente. Es cómodo entender como realización de G en $S(\Omega)$, cualquier homomorfismo $\Phi: G\to S(\Omega)$. Si Φ_g es una transformación de $S(\Omega)$, que responde al elemento $g\in G$, entonces, $\Phi = e_\Omega$ es la transformación unitaria $\Omega\to\Omega$ y $\Phi_{gh} = \Phi_g\circ\Phi_h$; $g, h\in G$. La imagen $\Phi_g(x)$ del punto (elemento) $x\in\Omega$ respecto a la transformación Φ_g frecuentemente se designa simplemente con el símbolo gh, lo que da lugar a hablar sobre las aplicaciones $(g, x)\mapsto gx$ del producto cartesiano (G, Ω) en Ω. Sería más correcto escribir $g\circ x$ o $g * x$, para que no hubiese confusiones con la multiplicación en G pero en la mayoría de los casos no es necesario. Las propiedades de la transformación Φ_g, antes señaladas, se escriben en la forma

(i) $\quad ex = x,\quad x\in\Omega,$

(ii) $\quad (gh)x = g(hx),\quad g,\ h\in G.$

Cada vez, cuando se tiene la aplicación $(g, x) \to gx$ del producto cartesiano $G \times \Omega$ en Ω, que satisface las propiedades (i), (ii), se dice que el grupo *opera* (a la izquierda), sobre el conjunto Ω, y que Ω es un *G-conjunto*. Por otra parte, teniendo un G-conjunto Ω, por medio de la fórmula

$$\Phi_g(x) = gx, \quad x \in \Omega,$$

definimos una aplicación $\Phi_g : \Omega \to \Omega$, para cada $g \in G$, además, de (i), (ii), se deduce, que $\Phi : g \mapsto \Phi_g$ será un homomorfismo de G sobre $S(\Omega)$. También se dice (en especial, cuando $|\Omega| < \infty$), que con la operación de G sobre Ω se asocia la *representación* (Φ, Ω) *del grupo G en el grupo de permutaciones*. El núcleo Ker Φ se llama *núcleo de operación* del grupo G. Si Φ es un monomorfismo (de otro modo: si $gx = x, \forall x \in \Phi \Rightarrow g = e$), entonces, se dice que el grupo G opera *efectivamente* sobre el conjunto Ω.

OBSERVACIÓN. Cada operación de G en Ω induce la operación de G en $\Omega^k = \Omega \times \ldots \times \Omega$ por la regla evidente: $g \cdot (x_1, \ldots, x_k) = (gx_1, \ldots, gx_k)$. Además, se tiene la operación inducida de G sobre el conjunto de todos los subconjuntos $\mathcal{P}(\Omega)$ (véase el ejercicio 4, § 5 del cap. 1). Hacemos $g\varnothing = \varnothing$, y si T es un subconjunto no vacío en Ω, entonces, $gT = \{gt \mid t \in T\}$. Las propiedades (i), (ii) se verifican inmediatamente. Es fácil comprender que T y gT tienen igual potencia, puesto que G indice la operación sobre los subconjuntos equipotentes.

2. **Orbitas y subgrupos estacionarios de puntos.** Dos puntos x, $x' \in \Omega$ se llaman equivalentes con relación al grupo G, que opera sobre Ω, si $x' = gx$ para algún elemento $g \in G$. Las propiedades de reflexibilidad, simetría y transitividad, obtenidas fácilmente con ayuda de (i), (ii) (véase el p. 1), muestran, que estamos en presencia de verdaderas relaciones de equivalencia, que dividen Ω en clases disjuntas de equivalencia. A estas clases de equivalencia se adopta llamarlas *G-órbitas*. La órbita contenedora del elemento $x_0 \in \Omega$, es natural designarla con el símbolo $G(x_0)$; de ese modo, $G(x_0) = \{gx_0 \mid g \in G\}$. También se emplean, sin embargo, otras notaciones, que subrayan las particularidades de una u otra operación de G en Ω. El concepto de órbita se tomó de la geometría. Si, por ejemplo, $G = \mathrm{SO}(2)$ es un grupo de rotaciones en un plano alrededor del punto de origen O, entonces, la circunferencia con centro en O, que pasa por P, servirá de órbita del punto P, y el conjunto $\Omega = \mathbb{R}^2$ será la unión de las circunferencias concéntricas, incluyendo la de radio nulo (el punto O). Para nosotros, el concepto de órbita tampoco es nuevo. Lo utilizamos en el cap. 4 para la descomposición de la permutación $\pi \in S_n$ en un producto de ciclos independientes. En calidad de G se tomó el grupo cíclico $\langle\pi\rangle$.

Sea x_0 un punto fijo en Ω. Examinemos el conjunto

$$\mathrm{St}(x_0) = \{g \in G \mid gx_0 = x_0\} \subset G.$$

Como $ex_0 = x_0$, y $g, h \in \mathrm{St}(x_0) \Rightarrow gh^{-1} \in \mathrm{St}(x_0)$, entonces, $\mathrm{St}(x_0)$ es un subgrupo en G. Este se denomina *subgrupo estacionario* (o *estabilizador*) en G del punto $x_0 \in \Omega$ y frecuentemente se anota con el símbolo G_{x_0}. Para la operación antes considerada del grupo SO (2) sobre $\mathbb{R}^2$ tenemos $\mathrm{St}(O) = \mathrm{SO}(2)$ y $\mathrm{St}(P) = e$, si $P \neq 0$. En el caso general

$$gx_0 = g'x_0 \Leftrightarrow g^{-1}g' \in \mathrm{St}(x_0) \Leftrightarrow g' \in g\,\mathrm{St}(x_0).$$

En consecuencia, las clases adjuntas para la izquierda $g\,\mathrm{St}(x_0)$ del grupo G respecto al subgrupo estacionario $\mathrm{St}(x_0)$, se encuentran en correspondencia biunívoca con los puntos de la órbita $G(x_0)$. En particular,

$$\mathrm{Card}\, G(x_0) = \mathrm{Card}\,(G/\mathrm{St}(x_0)) = (G : \mathrm{St}(x_0)). \qquad (1)$$

Aquí, como antes, $G/\mathrm{St}(x_0)$, es el conjunto cociente de G respecto a $\mathrm{St}(x_0)$, y $(G : \mathrm{St}(x_0))$ es el índice del subgrupo $\mathrm{St}(x_0)$ en G. La potencia $\mathrm{Card}\, G(x_0)$ muchas veces se llama *longitud de la G-órbita* del punto x_0.

De (1) y del teorema de Lagrange se deduce, que *la longitud de cualquier órbita con relación al grupo finito G, es divisor del orden del grupo.*

Prestemos también atención al hecho de que el punto x_0 en la parte derecha de las relaciones (1) puede ser sustituido por cualquier punto $x_0' \in G(x_0)$. En efecto,

$$\mathrm{Card}\, G(x_0) = \mathrm{Card}\, G(x_0') = (G : \mathrm{St}(x_0')).$$

Una afirmación más contundente sobre los subgrupos estacionarios consiste en lo siguiente. Sea $x_0' = gx_0$. Entonces

$$\mathrm{St}(x_0')gx_0 = \mathrm{St}(x_0')x_0' = x_0' = gx_0,$$

de donde

$$g^{-1}\mathrm{St}(x_0')\,gx_0 = x_0, \quad \text{o sea}, \quad g^{-1}\mathrm{St}(x_0')g \subset \mathrm{St}(x_0).$$

Análogamente,

$$g\,\mathrm{St}(x_0)g^{-1} \subset \mathrm{St}(x_0'),$$

por cuanto

$$\mathrm{St}(x_0)g^{-1}x_0' = \mathrm{St}(x_0)x_0 = x_0 = g^{-1}x_0'.$$

Esto significa, que tienen lugar las igualdades

$$\mathrm{St}(x_0') = g\mathrm{St}(x_0)g^{-1} = \{ghg^{-1} \mid h \in \mathrm{St}(x_0)\}.$$

En el espíritu del ejemplo 1, considerado más abajo, dos subgrupos $H, H' \subseteq G$ se llaman *conjugados*, si $H' = gHg^{-1}$ para algún $g \in G$. Expresemos los resultados obtenidos en forma de teorema:

TEOREMA 1. *Sea que el grupo G opera sobre el conjunto Ω. Si dos puntos $x_0, x_0' \in \Omega$ están situados en una órbita, entonces, los subgrupos*

estacionarios de ambos, son conjugados:

$$x'_x = gx_0 \Rightarrow \mathrm{St}\,(x_0)' = g\,\mathrm{St}\,(x_0)g^{-1}.$$

Si, luego, G es un grupo finito, y

$$\Omega = \Omega_1 \cup \Omega_2 \cup \ldots \cup \Omega_r$$

es una particulación de Ω en un número finito de órbitas con los representantes $x_1, x_2, \ldots, x_r$, entonces,

$$|\Omega| = \sum_{i=1}^{r} (G:\ \mathrm{ST}\,(x_i)) \quad \blacksquare \qquad (2)$$

La fórmula (2) sirve de base para muchos aplicaciones del «método de órbitas» a los grupos finitos.

3. Ejemplos de operaciones de los grupos en los conjuntos. Nos detendremos sólo en ejemplos, propiamente referidos a la teoría de los grupos.

EJEMPLO 1. (*operación por conjugación*). En $\Omega = G$ se define la operación de cualquier elemento $g \in G$ mediante la fórmula

$$x \to I_g\,(x) = gxg^{-1}, \quad \forall x \in G.$$

Se podría haber escrito $g \circ x = gxg^{-1}$, pero hemos preferido utilizar nuestra vieja notación del p. 2, § 3 cap. 4 para el automorfismo interno I_g, que corresponde al elemento $g \in G$.

La operación g, identificada con la operación $I_g \in \mathrm{Inn}\,(G)$, se llama por *conjugación* (o por *transformación*). Le sirve de núcleo el *centro* del grupo G:

$$Z\,(G) = \{z \in G \mid I_g\,(z) = z, \ \ \forall g \in G\} = \{Z \in G \mid zg = gz, \ \forall g \in G\}.$$

La órbita del elemento $x \in G = \Omega$, denotada aquí con el símbolo x^G, se llama *clase de elementos conjugados*, o sencillamente, *clase conjugada* contenedora de x. Si $a, b \in x^G$, entonces, a veces se escribe $a \underset{G}{\sim} b$. Para el subgrupo estacionario $\mathrm{St}\,(x)$, llamado en este caso *centralizador* del elemento x, con más frecuencia se emplea la denotación $C\,(x)$ (o $C_G\,(x)$, si en necesario separar el grupo G).

La operación por conjugación, de acuerdo con la observación al final del p. 1, se traslada a los subconjuntos y subgrupos en G. Dos subconjuntos $H, T \subset G$ son *conjugados*, si $T = gHg^{-1}$ para algún $n \in G$. Sea H un subgrupo en G. Se acostumbra decir, que

$$N\,(H) = \mathrm{St}\,(H) = \{g \in G \mid gHg^{-1} = H\}$$

es el *normalizador* del subgrupo H en G. En particular, $H \lhd G$ (H es un subgrupo normal en G), si $N\,(H) = G$, lo que está de acuerdo con las definiciones del cap. 4. En correspondencia con las relaciones (1), la *longitud de la órbita* H^G (*número de subgrupos conjugados con* H) *coincide con el índice del normalizador* $N\,(H)$ *en* G. $\blacksquare$

Sean, luego, G el grupo finito y $x_1^G, \ldots, x_r^G$, sus clases conjugadas, además, las q primeras de ellas son unielementales:

$$x_i^G = \{x_i\}, \quad i = 1, \ldots, q \ (x_1 = e).$$

Entonces, $Z(G) = \{x_1, x_2, \ldots, x_q\}$, y las relaciones (1) y (2) se reescriben en la forma

$$|x_i^G| = (G: C(x_i)); \tag{1'}$$

$$|G| = |Z(G| + \sum_{i=q+1}^{r} (G:C(x_i)). \tag{2'}$$

Sea, digamos, $G = S_3$. Entonces, $r = 3$, $q = 1$ (o sea, $Z(S_3) = e$) y

$$S_3 = \{e\} \cup \{(12), (13), (23)\} \cup \{(123), (132)\}$$

es la partición de S_3 en clases conjugadas. Las dimensiones de estas clases (longitudes de las órbitas) dividen al $6 = |S_3|$, como lo prescribe la relación (1'). La relación (2') conduce inmediatamente a la siguiente afirmación interesante.

TEOREMA 2. *Cualquier p-grupo finito G (grupo de orden $p^n > 1$, p es un número primo) posee un centro $Z(G) \neq e$.*

DEMOSTRACIÓN. Si G es un grupo abeliano, entonces, $G = Z(G)$ y no hay nada que demostrar. En caso contrario $r > q$, $(G : C(X_i)) = p^{n_i}$, $n_i \geqslant 1$ cuando $i > q$, y la relación (2), reescrita en la forma

$$p^n = |Z(G)| + \sum_{i=q+1}^{r} p^{n_i},$$

muestra, que $|Z(G)|$ se divide por p. ∎

La existencia del p-grupo no abeliano es fácil de establecer. Es suficiente examinar el grupo de las matrices triangulares superiores

$$P = \left\{ \left\| \begin{matrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{matrix} \right\| \, \middle| \, a, b, c \in Z_p \right\}$$

con coeficientes en un campo finito de p elementos.

EJEMPLO 2. (*traslación*). La aplicación $L_a: G \to G$, definida por la fórmula $L_a(g) = ag$, que utilizamos en la demostración del teorema de Cayley (véase el § 3 del cap. 4), con frecuencia es llamada *traslación por la izquierda* en a. Como $eg = g$ y $(ab)g = a(bg)$, entonces, las traslaciones por la izquierda provocan la operación de G en sí mismo, y ésta induce la operación en los subconjuntos del grupo G. Sean, en particular, H el subgrupo y G/H el conjunto de las clases adjuntas por la izquierda respecto a gH, $g \in G$.

Es claro, que la aplicación

$$(x, gH) \to g(gH) = xg)H$$

determina la operación L^H del grupo G en G/H. El núcleo Ker L^H de esta operación es el conjunto $\{x \in G \mid L_x^H (gH) = gH, \forall g \in G\} = \{x \in G \mid L_x^H (gH) = gH, \forall g \in G\} = \{x \in G, xgH = gH, \forall g \in G\}$.
Con otras palabras, $x \in \operatorname{Ker} L^H \Leftrightarrow g^{-1}xg \in H$ para todas $g \in G$ o, lo que es equivalente, $x \in gHg^{-1}$, $\forall g \in G$.

De este modo,

$$\operatorname{Ker} L^H = \bigcap_{g \in G} fHf^{-1}$$

es el mayor subgrupo normal del grupo G, contenido en H. La efectividad de la operación de G en G/H es equivalente a la ausencia del subgrupo $K \subset H$, $K \neq e$, normal en G.

En todo caso, cualquier subgrupo H de índice n en G puede usarse para la representación $(L^H, G/H)$ del grupo G con permutaciones L_x^H en las clases adjuntas G respecto a H. Esta representación (posiblemente, no exacta) es mucho más económica que la obtenida mediante el empleo del teorema de Cayley.

EJEMPLO 3. (*grupos transitivos*). El grupo de las permutaciones $G \subset S_n$, que opera en el conjunto $\Omega = \{1, 2, \ldots, n\}$, se llama *transitivo*, si la órbita G_i de algún (en consecuencia, cualquier) punto $i \in \Omega$ coincide con Ω. Con otras palabras, la operación $G \times \Omega \to \Omega$ es *transitiva* en Ω cuando para cada par de puntos $i, j \in \Omega$ se halla por lo menos un elemento $g \in G$ con $g(i) = j$.

Sea $\Omega^{[k]}$ una colección de subconjuntos k-elementales ordenados en Ω. El grupo G, que opera en Ω, induce la operación en $\Omega^{[k]}$; si, además, tiene lugar la transitividad en $\Omega^{[k]}$, entonces G, se llama *k-transitivo* en Ω. Digamos, el grupo simétrico S_n es n-transitivo en Ω, y el grupo alternativo A_n, es $(n - 2)$ — transitivo.

Cualquier grupo G opera con transitividad en el conjunto G/H de las clases adjuntas por la izquierda G respecto a H (véase el ejemplo 2). Efectivamente, si g_iH, g_jH son clases adjuntas, entonces, $g_jg_i^{-1}(g_iH) = g_jH$. Con más razón es sorprendente, que sobre los grupos k-transitivos para $k > 5$ se sabe muy poco. Existe incluso una hipótesis de C. Jordan (no demostrada) de hace más de un siglo, que tales grupos son sólo dos: S_n y A_n.

Nos disponemos a obtener curiosos resultados cuantitativos sobre los grupos transitivos, que nos serán necesarios en adelante. Sea G un grupo transitivo en Ω. El grupo estacionario St (i) del punto $i \in \Omega$ lo designamos con el símbolo G_i. Sabemos (véase el teorema 1), que si $i = g_i(1)$: entonces, $G_i = g_iG_1g_i^{-1}$, $i = 1, 2, \ldots, n$ $(g_1 = e)$. Además, se puede tomar los elementos g_i en calidad de representantes de las clases adjuntas por la izquierda G respecto a G_1:

$$G = G_1 \cup g_2G_1 \cup \ldots \cup g_nG_1. \quad (3)$$

En particular, $|G| = n\,|G_1|$, lo que concuerda con los resultados generales sobre las longitudes de las órbitas (véase el p. 2).

TEOREMA 3. *Sea G un grupo transitivo en Ω, y, para cualquier $g \in G$ sea $N(g)$ el número de puntos en Ω, que quedan en sus lugares para la operación de g. Entonces:*

(i) $\sum_{g \in G} N(g) = |G|$ *(dividiendo ambos miembros de la igualdad (i) por $|G|$, obtenemos, que «en promedio» cada elemento deja fijo un punto);*

(ii) *si G es un grupo 2-transitivo, entonces,*

$$\sum_{g \in G} N(g)^2 = 2\,|G|.$$

DEMOSTRACION. (i). Tenemos.

$$\sum_{g \in G} N(g) = \sum_{j=0}^{n} \Gamma(j),$$

dondo $\Gamma(j)$ es el número de elementos en G, que dejan el símbolo j en su lugar. Con otras palabras, $\Gamma(j) = |G_j|$. Pero, en virtud de la transitividad $|G_j| = |g_j G_1 g_j^{-1}| = |G_1|$, donde g_j se han tomado de la descomposición (3). En consecuencia.

$$\sum_{g \in G} N(g) = \sum_{j=1}^{n} |G_j| = \sum_{j=1}^{n} |G_1| = n\,|G_1| \parallel |G|.$$

(ii) La condición de 2-transitividad de G significa, que en el conjunto $\Omega_1 = \Omega \diagdown \{1\}$ el subgrupo estacionario G_1 opera con transitividad, o sea, las G_1-órbitas serán $\{1\}$ y Ω_1. Sea $N'(x)$ el número de puntos en Ω_1, inmóviles durante la operación $x \in G_1$. La relación (i) empleada en el par (G_1, Ω_1), da

$$\sum_{x \in G_1} N'(x) = |G_1|.$$

Como $N(x) = 1 + N'(x)$ para $x \in G_1$ (se agrega el punto 1), entonces, tenemos

$$\sum_{x \in G_1} N(x) = 2\,|G_1|\cdot$$

Iguales relaciones son válidos para todos los restantes G_j: Sumando con respecto a j, obtenemos

$$\sum_{j=1}^{n} \sum_{x \in G_j} N(x) = 2n\,|G_1| = 2\,|G|.$$

A la izquierda $N(x)$ se considera de a uno para cada subgrupo G_j, que contiene a x. Pero, x deja en sus lugares $N(x)$ puntos y, por consiguiente, está contenida exactamente en $N(x)$ subgrupos G_j. Esto significa, que cada elemento x aporta a la suma el término $N(x)^2$. Por otra parte, cualquier elemento $y \in G$, no contenido en la unión $\bigcup_j G_j$, permuta todos los puntos, así que $N(y) = 0$. Por

eso, se puede escribir la relación

$$\sum_{g\in G} N(g)^2 = \sum_{i=1}^{n} \sum_{x\in G_j} N(x) = 2|G|. \quad \blacksquare$$

4. **Espacios homogéneos.** Para la geometría tiene especial interés el caso, cuando Ω es un espacio topológico (por ejemplo, la recta $\mathbb{R}$ o la esfera S^2), G es un grupo llamado, continuo (o topológico), y la operación $(g, x) \to gx$ se somete a la exigencia razonable:

(iii) $f(g, x) = gx$ es función continua de dos variables g y x. El grupo G, que opera en Ω de tal modo que se cumplen las propiedades (i), (ii) del p. 1 y la (iii), se llama *grupo de movimientos* del espacio Ω. Con esto, pueden haber movimientos que conserven alguna métrica en Ω. El espacio Ω se llama *homogéneo*, si G opera en Ω transitivamente en el sentido del ejemplo 3, o sea, si todos los puntos de Ω pertenecen a una G-órbita.

De los razonamientos generales de los puntos 1 y 2 es claro, que se tiene correspondencia biunívoca entre los puntos del espacio homogéneo Ω y las clases adjuntas G respecto a uno de los subgrupos estacionarios H. Además, al movimiento $g \in G$ del espacio Ω le corresponde la aplicación $g'H \to gg'H$ en el conjunto G/H.

Examinemos desde un nuevo punto de vista el ejemplo del grupo $SO(3)$, que conocemos bien del § 1. Es cómodo para el grupo $SO(3)$ representarse como operando en la esfera bidimensional S^2 de radio unidad. Evidentemente, a cualquier par de puntos $P, Q \in S^2$ le corresponde algún movimiento (rotación), que traslada P a Q, sea, S^2 es un espacio homogéneo con el grupo de movimientos $SO(3)$. El subgrupo estacionario $St(P)$ de cualquier punto $P \in S^2$ deja inmóvil todo el eje que pasa por P y por el centro O de la esfera. Por eso, $St(P) \cong SO(2)$ es un grupo de rotaciones del plano perpendicular al eje OP.

Como los elementos del grupo $SO(2)$ se identifican con los puntos de la circunferencia S^1 de radio unidad, entonces, el grupo $SO(3)$ puede representarse en forma de pastel hojaldrado, cuyas capas con círculos unidades, «numerados» con los puntos de la esfera bidimensional $SO(3)/S^1 \approx S^2$. En este caso se habla sobre *la estratificación* (o proyección de p: $SO(3) \to S^2$) con *base* S^2 y *estrato* $p^{-1}(P) \approx S^1$, $P \in S^2$. El sentido exacto de todos estos conceptos se explica en los cursos de geometría y topología, por eso nos limitamos a lo expresado.

EJERCICIOS

1. Sean Φ y Φ', homomorfismos del grupo G sobre $S(\Omega)$ y $S(\Omega')$, respectivamente. Entonces, las operaciones definidas por los mismos en Ω y en Ω' se llaman *equivalentes*, si existe la aplicación biyectiva σ: $\Omega \to \Omega'$ que hace conmutativo el diagrama

$$\begin{array}{ccc} \Omega & \xrightarrow{\sigma} & \Omega' \\ \Phi_g \downarrow & & \downarrow \Phi'_g \\ \Omega & \xrightarrow{\sigma} & \Omega' \end{array}$$

para todo $g \in G$. De este modo, $\Phi'_g = \sigma\Phi_g\sigma^{-1}$. Demostrar, que cada operación transitiva del grupo G es equivalente a la operación de G en las clases adjuntas por la izquierda respecto a algún subgrupo H. (*Indicación*. Tomar en calidad de H el subgrupo estacionario G_1 del punto $1 \in \Omega$, utilizar la descomposición (3) y hacer $\sigma(i) = g_iG_1$.)

2. Haciendo hincapié en el teorema 2, demostrar, que todos los grupos de orden p^2 (p es número primo) son abelianos.

3. Mostrar, que el centro del grupo P, citado al final del ejemplo 1, tiene la forma

$$Z(P)=\left\{\left\|\begin{matrix}1 & 0 & c\\ 0 & 1 & 0\\ 0 & 0 & 1\end{matrix}\right\| \mid c\in Z_p\right\}.$$

Hallar las clases conjugadas del grupo P (*Indicación.* Tener en cuenta, que todos los elementos del grupo P tienen la forma

$$g=A^iB^jC^k,\quad \text{donde}\quad A=\left\|\begin{matrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{matrix}\right\|,\quad B=\left\|\begin{matrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{matrix}\right\|,\quad C=\left\|\begin{matrix}1 & 0 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{matrix}\right\|;$$

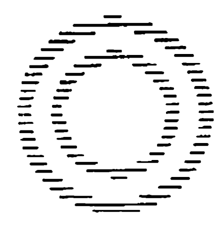
si $g\notin Z(P)$, entonces, $C_P(g)=\langle g\rangle Z(G)$, $|C_P(g)|=p^2$.)

4. Sea n un número natural. Escribámoslo en forma de la suma $n=n_1+n_2+\ldots+n_m$ con $n_1\geqslant n_2\geqslant\ldots n_m\geqslant 1$. El número de todas estas particiones con $m=1, 2, \ldots$ lo designamos por medio de $p(n)$, de tal modo que $p(3)=3$, $p(4)=5$, etc. La descomposición $\pi=\pi_1\pi_2\ldots\pi_m$ de cada permutación $\pi\in S_n$ en el producto de los ciclos independientes (véase el § 2 del cap. 4) determina unívocamente la partición del número n. Mostrar, que las clases conjugadas del grupo S_n se hallan en correspondencia biyectiva con las particiones del número n. (*Indicación.* Si $\sigma\in S_n$ y $\pi=\pi_1\ldots\pi_m$, entonces, $\sigma\pi\sigma^{-1}=\sigma\pi_1\sigma^{-1}\ldots\sigma\pi_m\sigma^{-1}$; luego, $\sigma\cdot(i_1i_2\ldots i_k)\cdot\sigma^{-1}=(\sigma(i_1)\,\sigma(i_2)\ldots\ldots\sigma(i_k))$ para cualquier ciclo $(i_1i_2\ldots i_k)$ de longitud k).

5. Sea que la permutación $\pi\in S_n$ se escribe en forma de producto de r ciclos de longitud 1, s ciclos de longitud 2, t ciclos de longitud 3, etc., así que $n=r+2s+3t+\ldots$ Mostrar, que la potencia de la clase conjugada en S_n, que contiene la permutación π, se expresa por la fórmula

$$|\pi^{S_n}|=\frac{n!}{1^r r!\,2^s s!\,3^t t!\ldots}.$$

6. Sea que el grupo G opera en el conjunto Ω. Llamemos al subconjunto $\Gamma\subset\Omega$ *invariante* respecto a G (o G—*invariante*), si $g^x\in\Gamma$ para todo $g\in G$ y $x\in\Gamma$. Por ejemplo, con las operaciones $SO(2)\times\mathbb{R}^2\to\mathbb{R}^2$, resultan conjuntos



invariantes los anillos concéntricos. Mostrar, que cualquier subconjunto invariante respecto a Ω es una unión de órbitas, además, la G—órbita de cualquier elemento $x\in\Omega$ no es otra cosa que el menor subconjunto invarian e, contenedor de x.

7. Mostrar, que para el grupo G con subgrupo H, la operación $H\times G\to G$, definida por la traslación $(h, g)\mapsto hg$, da una partición de G en clases adjuntas por la derecha G con relación a H.

8. Modificando la demostración del teorema 1, obtener la relación

$$r(G:\Omega)=\frac{1}{|G|}\sum_{g\in G}N(g),$$

donde $r(G:\Omega)$ es el número de órbitas del grupo de permutaciones G que opera en el conjunto Ω. (*Indicación*. En la suma $\sum N(g)$ cada elemento $x \in \Omega$ se cuenta $|St(x)|$ veces. Por lo tanto, los elementos que están en una misma órbita que x, efectúan un aporte en $\sum N(g)$, igual a $(G:St(x)) \times |St(x)| = |G|$).

§ 3. ALGUNAS ESTRUCTURAS TEORICO-GRUPALES

Este parágrafo, en especial el p. 1, presenta algunas dificultades, y al mismo hay que regresar repetidas veces, para asimilar en ejemplos concretos un pequeño número de conceptos abstractos.

1. Teoremas generales sobre los homomorfismos de grupos. Vimos en el § 4 del cap. 4, que a cada subgrupo normal K del grupo G se asocia cierto nuevo grupo G/K, que fue llamado grupo cociente del grupo G respecto a K. Así, junto con el epimorfismo Φ: SU $(2) \to$ SO (3), descrito en el § 1, es natural introducir el grupo cociente SU $(2)/\{\pm E\}$ y compararlo con la imagen Im Φ = SO (3). Es fácil darse cuenta, que SU $(2)/\{\pm E\} \cong$ SO (3), pero, para no repetir cada vez los razonamientos, es útil establecer una serie de hechos comunes, sobre los subgrupos, homomorfismos y grupos cocientes. En adelante, la escritura $K \lhd G$ significa, que K es un subgrupo normal en G.

TEOREMA 1. (teorema fundamental sobre los homomorfismos). *Sea $\varphi: G \to H$ un homomorfismo de los grupos con núcleo K =* Ker φ. *Entonces, K es un subgrupo normal en G* y $G/K \cong$ Im φ. *Recíprocamente, si $K \lhd G$, entonces, existen un grupo H (precisamente, G/K) y el epimorfismo $\pi: G \to H$, cuyo núcleo coincide con K (π frecuentemente se llama aplicación natural* u *homomorfismo natural*).

DEMOSTRACIÓN. Ya sabemos, que Ker $\varphi = K \lhd G$. Definemos la aplicación $\bar\varphi: G/K \to H$, haciendo

$$\bar\varphi(gK) = \varphi(g).$$

Si $g_1K = g_2K$, entonces, $g_1^{-1}g_2 \in K$, $\varphi(g_1^{-1}g_2) = e$ y, en consecuencia, $\varphi(g_1) = \varphi(g_2)$, y esto significa, que la aplicación $\bar\varphi$ está definida correctamente (o sea, no depende de la elección del representante de la clase adjunta). Como $\bar\varphi(g_1K \cdot g_2K) = \bar\varphi(g_1g_2K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \bar\varphi(g_1K)\,\bar\varphi(g_2K)$, entonces, $\bar\varphi$ es un homomorfismo. Efectivamente, $\bar\varphi$ es un monomorfismo, porque de $\bar\varphi(g_1K) = \bar\varphi(g_2K)$ se deduce $\varphi(g_1) = \varphi(g_2)$, de donde $\varphi(g_1^{-1} \times g_2) = e$, $g_1^{-1}g_2 \in K$ y $g_1K = g_2K$. Es también que claro, que Im $\bar\varphi$ = Im φ. Por eso, $\bar\varphi$ resulta el hisomorfismo buscado G/K en la Im φ.

Recíprocamente, sea $K \lhd G$. Tomemos en calidad de π la función que confronta a cualquier elemento de G su clase adjunta respecto a K, o sea, hagamos $\pi(g) = gK$. Es claro, que todas las propiedades exigidas se cumplen. ∎

Corresponde observar, que prefijando el núcleo, el homomorfismo se determina no unívocamente. Por ejemplo, los automorfismos $g \mapsto g$ y $g \mapsto g^{-1}$ de un grupo abeliano de orden primo $p > 2$ son diferentes, pero sus núcleos coinciden ($=e$).

Teniendo el homomorfismo $\rho: G \to G_1$ y el subgrupo $H \subset G$. es natural echarle una mirada a la limitación ρ_H y a la imagen del subgrupo H con relación a este homomorfismo. El teorema siguiente, simplifica considerablemente el análisis de todas las situaciones posibles.

TEOREMA 2 (primer teorema sobre el isomorfismo). *Sean, el grupo G y sus subgrupos H y K, además, K es normal en G. Entonces, $HK = KH$ es un subgrupo en G, contenedor de K. Luego, la intersección $H \cap K$ es un subgrupo normal en H, y la aplicación*

$$\varphi : hK \mapsto h(H \cap K)$$

es un isomorfismo de los grupos:

$$HK/K \cong H/H \cap K.$$

DEMOSTRACIÓN. La condición $K \lhd G$, reescrita en la forma $gK = Kg$, $g \in G$, significa, en particular, que $hK = Kh$ para todo $h \in H$. El conjunto $HK = \{hk \mid h \in H, k \in K\}$ se compone de un cierto número de clases adjuntas hK : $HK = \bigcup_{h \in H} hK$. Sustituyendo aquí hK por Kh, llegamos a la igualdad

$$HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH.$$

Es evidente, que el elemento unidad e, contenido en H y K, también se contiene en HK. Luego, $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hkh^{-1})^{-1} \in HK$, por eso, los inversos de todos los elementos de HK, se encuentran en HK. Finalmente, $HK \times HK = H \cdot KH \cdot K = H \cdot HK \cdot K = HK$, o sea, el conjunto HK es cerado con respecto a la multiplicación. Vemos, que el subconjunto $HK \subset G$ es un subgrupo en G.

Como $K \subset HK$ y $K \lhd G \Rightarrow K \lhd HK$, entonces, tiene sentido hablar sobre el grupo cociente HK/K. Sean, $\pi: G \to G/K$ un epimorfismo natural y, $\pi_0: \pi|_H$ la limitación de π en H. Su imagen $\operatorname{Im} \pi_0$ está compuesta de las clases adjuntas hK, $h \in H$, o sea, de todas las clases adjuntas de G respecto a K, qu tienen representantes en H Con otras palabras, $\operatorname{Im} \pi_0 = HK/K$. Y bien, tenemos el epimorfismo

$$\pi_0 : H \to HK/K.$$

Su núcleo $\operatorname{Ker} \pi_0$ se compone de $h \in H$, para los cuales $\pi_0(h) \equiv hK = K$ es unidad en HK/K. Pero, $hK = K \Leftrightarrow h \in H \cap K$, de donde, $\operatorname{Ker} \pi_0 = H \cap K$. Como cualquier núcleo de homomorfismo, $H \cap K$ es subgrupo normal en H (esto, sin esfuerzo, se comprueba inmediatamente).

Según el teorema fundamental sobre homomorfismos (teorema 1) la correspondencia $\overline{\pi}_0 : h(H \cap K) \to \pi_0(h) = hK$, establece el isomorfismo $H/H \cap K \cong HK/K$. Como $\overline{\pi}_0$ es una aplicación biyectiva, entonces, $\varphi = \overline{\pi}_0^{-1} : hK \to h(H \cap K)$ también es isomorfismo de los grupos HK/K y $H/H \cap K$. ∎

Ya que se tiene un primer teorema sobre el isomorfismo, deberá existir un segundo. Así es, pero formularemos su variante simplificada, que tiene un nombre especial.

TEOREMA 3. (teorema sobre la correspondencia). *Sean, el grupo G y sus subrrupos H y K, además, $K \lhd G$ y $k \subset H$. Entonces, $\overline{H} = H/K$ es un subgrupo en $\overline{G} = G/K$ y π^*: $H \to \overline{H}$ es una aplicación biyectiva del conjunto $\Omega(G, K)$ de los subgrupos en G, contenedores de K, sobre el conjunto $\Omega(\overline{G})$ de todos los subgrupos del grupo $\overline{G}$. Si $H \in \Omega(G, K)$, entonces, $H \lhd G \Leftrightarrow \overline{H} \lhd \overline{G}$, además*

$$G/H \cong \overline{G}/\overline{H} = (G/K)/(H/K).$$

DEMOSTRACION. Sea $H \in \Omega(G, K)$. De la definición de G/K surge inmediatamente que H/K es un subgrupo en G/K. A fin de convencerse de la inyectividad de la aplicación $\pi^* : H \to \overline{H}$, examinemos dos subgrupos $H_1, H_2 \in \Omega(G, K)$, para los cuales $H_1/K = H_2/K$. Entonces, $h_1 \in H_1 \Rightarrow h_1K = h_2K$, $h_2 \in H_2 \Rightarrow h_1 = h_2k$, y, como $K \subset H_2$, entonces, $h_1 \in H_2$, de donde, $H_1 \subset H_2$. Análogamente se comprueba la inclusión $H_2 \subset H_1$. Por lo tanto. $H_1 = H_2$.

Establecemos ahora la sobreyectividad de la aplicación π^*. Sean, $\overline{H} \in \Omega(\overline{G})$ y H el conjunto de tales elementos en G, de los cuales se componen todas las clases adjuntas respectoa K, que son elementos del grupo $\overline{H} \subset \overline{G}$. Entonces, en particular, $K \subset H$ y $a, b \in H \Rightarrow aK$, $bK \in \overline{H} \Rightarrow abK = aKbK \in \overline{H} \Rightarrow ab \in H$ y $a \in H \Rightarrow aK \in \overline{H} \Rightarrow a^{-1}K = (aK)^{-1} \in \overline{H} \Rightarrow a^{-1} \in H$. Por lo tanto H es un subgrupo en G, además, $\overline{H} = H/K$ (por lo común, H se llama *preimagen* en G del subgrupo $\overline{H} \in \overline{G}$).

Es suficientemente evidente la iplicación $H \in \Omega(G, K)$, $H \lhd G \Rightarrow \overline{H} \lhd \overline{G}$, que se deduce formalmente de las igualdades $gK \cdot hK \cdot (gK)^{-1} = ghg^{-1}K = h'K \in \overline{H}$ para todo $g \in G$, $h \in H$. Pero, por las mismas razones $\overline{H} \lhd \overline{G} \Rightarrow ghg^{-1}K = gK \cdot hK \cdot (gK)^{-1} = h'K \Rightarrow ghg^{-1} \in H \Rightarrow H \lhd G$.

Finalmente, en la situación $H \in \Omega(G, K)$, $H \lhd G$, según lo demostrado, se pueden examinar dos epimorfismos naturales

$$\pi : G \to G/K; \ \overline{\pi} : \overline{G} \to \overline{G}/\overline{H}$$

$(\overline{\pi}(\overline{g}) = \overline{g}\overline{H}$, donde $\overline{g} = gK \in (\overline{G})$ y la composición de los mismos es el epimorfismo

$$\sigma = \overline{\pi} \circ \pi = G \to \overline{G}/\overline{H},$$

definido por la regla $\sigma(g) = \overline{\pi}(\overline{g}) = \overline{g}\overline{H}$. Tenemos: $\operatorname{Ker} \sigma =$ $= \{g \in G \mid \sigma(g) = \overline{H}\} = \{g \in G \mid \overline{g} \in \overline{H}\} = \{g \in G \mid gK = hK$ para algún $h \in H\} = H$. En consecuencia, según el teorema fundamental sobre los homomorfismos, la aplicación, $gH \to \overline{gH}$ resulta un isomorfismo entre G/H y $\overline{G}/\overline{H}$. ▮

EJEMPLO 1 Sea $n = dm$ un número natural con divisor $d > 1$. Evidentemente, $n\mathbb{Z} \subset d\mathbb{Z}$ y la aplicación $x \mapsto dx + n\mathbb{Z}$ es un epimorfismo de los grupos aditivos:

$$\mathbb{Z} \to d\mathbb{Z}/n\mathbb{Z} = \{dt + n\mathbb{Z} \mid t = 0, 1, \ldots, m-1\}$$

con núcleo $m\mathbb{Z}$. Según el teorema 1 tenemos el isomorfismo

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z}$$

(lo que ya está lo suficientemente claro). Con ayuda del teorema 3 hallamos

$$\mathbb{Z}/d\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}), \quad \text{o sea,} \quad Z_d \cong Z_n/Z_m.$$

Recordando el teorema 5, § 3, cap. 4, llegamos a la afirmación, de que *todos los subgrupos y grupos cocientes de un grupo cíclico también son grupos cíclicos.*

Este resultado puede obtenerse, es claro, prescindiendo del teorema sobre los homomorfismos.

EJEMPLO 2. En el grupo simétrico S_4, separemos los subgrupos:
$V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \lhd S_4$ (véase el ejercicio 4 del § 2).
$S_3 = \{e\,(12), (13), (23), (123), (132)\}$
(en este caso, S_3 es el subgrupo estacionario del punto $i = 4$). Como, evidentemente, $S_3 \cap V_4 = e$, entonces, según el teorema 2, para el subgrupo $H =$ $= S_3V_4$, tenemos

$$H/V_4 \cong S_3/S_3 \cap V_4 \cong S_3.$$

En particular, $|H| = |V|_4 |S_3| = 24$, o sea, $H = S_4$. Y bien, S_4 posee un subgrupo, isomorfo a S_3 y análogo al grupo cociente. Empleando el teorema 3, obtenemos la descripción del conjunto $\Omega(S_4, V_4)$ de los subgrupos en S_4, contenedores de V_4:
$\Omega(S_4V_4) = \{V_4\ \langle(12)\rangle V_4, \langle(13)\rangle V_4, \langle(23)\rangle V_4, A_4 = \langle(123)\rangle V_4, S_4\}$.
Prestemos atención al hecho de que para cualquier divisor d del número 24 en S_4 se tiene por lo menos un subgrupo de orden d. En particular, existen exactamente cuatro subgrupos $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$, $\langle(234)\rangle$ de orden 3 y tres subgrupos $\langle(2)\rangle V_4$, $\langle(13)\rangle V_4$, $\langle(23)\rangle V_4$ de orden 8 (los llamados subgrupos 3-sílov y 2-sílov). Los propios grupos normales (o sea, $\neq e$ y S_4) son sólo dos: V_4 y A_4.

Efectivamente, si $K \lhd S_4$ y $K \cap V_4 \neq e$, entonces, $K \supset V_4$, porque los elementos no unitarios en V_4 son todos conjugados con relación a S_4. Dirigiéndose al conjunto $\Omega(S_4, V_4)$ vemos, que $K = V_4$ ó A_4. Y si $K \cap V_4 = e$, $K \neq e$, entonces

$$K \rhd S_4, \ V \rhd S_4 \Rightarrow kV_4 \rhd S,$$

y sólo que a aceptar, que $KV_4 = S_4$, $K \cong S_3$. Pero, S_3 contiene una trasposición, y todas las trasposiciones son conjugadas en S_4 y engendran S_4. Por otra

parte, ellas deben estar contenidas en K. La contradicción obtenida muestra que el caso $K \cap V_4 = e$ es imposible.

2. Grupos resolubles. La expresión

$$[x, y] = xyx^{-1}y^{-1},$$

llamada *conmutador* de los elementos x, y del grupo G, sirve de término corrector, necesario para cambiar los lugares de x e y:

$$xy = [x, y]\, yx.$$

Si x e y son permutables, entonces, $[x, y] = e$. Es intuitivamente claro, que, cuanto más conmutadores diferentes de e haya en el grupo G, tanto más significativa será la desviación de la ley de multiplicación en G de la conmutativa. Sea M el conjunto de todos los conmutadores en G. Se llama *conmutante* (o *subgrupo derivado*) del grupo G el subgrupo G' $(= G^{(1)} = [G, G])$, engendrado por el conjunto M (véase el p. 2, § 2, cap. 4):

$$G' = \langle [x, y] \mid x, y \in G \rangle.$$

Aunque $[x, y]^{-1} = yxy^{-1}x^{-1} = [y, x]$ es un conmutador, el producto de dos conmutadores no necesariamente lo es, así G' se compone de todos los productos posibles del tipo de

$$[x_1, y_1]\,[x_2, y_2] \ldots [x_k, y_k] \text{ con } x_i, y_i \in G.$$

Por supuesto, en cada caso concreto es deseable tener la descripción más exacta del conmatuante G'.

EJEMPLO. $G = S_n$. El conmutador $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$ de os permutaciones cualesquiera α, $\beta \in S_n$ es, evidentemente, una permutación par. Por eso $S'_n \subset A_n$. Luego,

$$(ij)\,(ik)\,(ij)^{-1}\,(ik)^{-1} = (ij)\,(ik)\,(ij)\,(ik) = (ijk),$$

como con los ciclos triples(ijk) se engendra todo el grupo alternativo A_n (véase el ejercicio 8, § 2 cap. 4), entonces, llegamos a la conclusión de que $S'_n = A_n$.

Observemos, que $S'_n \triangleright S_n$ y el grupo ociete S_n/S'_n es abeliano.

Volviendo al caso general, consideremos el homomorfismo arbitrario de grupos $\varphi\colon G \to \bar{G}$. Como

$$\varphi([x, y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\,\varphi(x)^{-1}\,\varphi(y)^{-1} = [\varphi(x), \varphi(y)]$$

entonces, $\varphi(G') \subset (\bar{G})'$, además, $\varphi(G') = (\bar{G}')$, si φ es un epimorfismo. Sea ahora K un subgrupo normal en G, y $\varphi = I_a\colon x \to axa^{-1}$ un automorfismo interno del grupo G, que induce algún endomorfismo en K. De acuerdo con lo dicho antes $I_a(K') \subset K'$ para cualquier $a \in G$ y esto significa, que

$$K \lhd G \Rightarrow K' \lhd G. \qquad (1)$$

En particular, $G' \lhd G$. Demostremos ahora una afirmación general que revela el sentido intrínseco del concepto de conmutante.

TEOREMA 4. *Cualquier subgrupo $K \subset G$, contenedor del conmutante G' del grupo G es normal con respecto a G. El grupo cociente G/G' es abeliano y G' está contenido en cada subgrupo normal K, tal, que G/K es abeliano (en particular, el orden máximo del grupo cociente abeliano G/K es igual al índice $(G : G')$.*

DEMOSTRACION. Si $x \in K$, $g \in G$ y $G' \subset K$, entonces, $gxg^{-1} = (gxg^{-1}x^{-1})x = [g, x]\, x \in G'/K = K$, así que $K \lhd G$. Luego, de las condiciones $G' \subset K$, $K \lhd G$, cumplidas, en particular, cuando $K = G'$ (véase (1)), se deduce que

$$[aK, bK] = aK \cdot bK \cdot a^{-1}K \cdot b^{-1}K = aba^{-1}b^{-1}K = [a, b]K = K,$$

o sea, el conmutador de cualesquiera dos elementos del grupo cociente G/K es igual al elemento unidad $(=K)$. Por lo tanto, G/K es un grupo abeliano. Recíprocamente, si $K \lhd G$ y el grupo cociente es abeliano, entonces

$$[a, b]K = [aK, bK] = K$$

para todo $a, b \in G$. Por consiguiente, $[a, b] \in K$ y $G' \subseteq K$ por cuanto G' es engendrado por los conmutadores. ∎

OBSERVACIÓN. Ahora conocemos dos subgrupos normales importantes de cualquier grupo G: el centro $Z(G)$ y el conmutante G'. La relación entre ellos, hablando en general, es débil, pero la ley común es ésta: cuanto más «cerca» está G de ser un grupo abeliano, tanto mayor es $Z(G)$ y menor G'. Es de mayor interés el hecho siguiente.

El grupo cociente $G/Z(G)$ del grupo no abeliano G respecto al centro $Z(C)$, no puede ser cíclico.

En efecto, si $G/Z(G)$ es un grupo cíclico, entonces, $G = \bigcup_i a^i Z(G)$ y cualquier elemento de G tiene la forma $g = a^i z$, $z \in Z(G)$. En tal caso $[g, h] = [a^i z, a^j z'] = a^{i+j-i-j}[z, z'] = e$ para cualesquiera dos elementos $g, h \in G$, $G' = e$ y G es un grupo abeliano, pese a lo supuesto.

En G' también se puede examinar el conmutante $(EG')' = G''$, llamado *grupo derivado segundo* (*segundo conmutante*) del grupo G. Continuando este proceso, definimos el grupo derivado k-ésimo $G^{(k)} = (G^{(k-1)})'$. De acuerdo con (1), $G^{(k)} \lhd G$ y, con más razón, $G^{(k)} \lhd G^{(k-1)}$. Se obtine la serie de subgrupos normales

$$G \rhd G^{(1)} \rhd G^{(2)} \rhd \ldots \rhd G^{(k)} \rhd G^{(k+1)} \rhd \ldots$$

con los grupos cocientes abelianos $G^{(k)}/G^{(k+1)}$.

El grupo G se llama *resoluble*, si la serie (2) se interrumpe en el subgrupo unidad, o sea, $G^{(m)} = e$ para algún índice mínimo de m *grados de solubilidad* del grupo G. Es evidente, que cualquier grupo abeliano, entre ellos también los cíclicos, es resoluble de grado 1.

Además, en cualquier grupo resoluble G de grado de solubilidad m, se tiene un subgrupo abeliano normal $\neq e$, precisamente $G^{(m-1)}$. Como muestran los ejemplos examinados, $S_4' = A_4$, $A_4' = V_4$, $V_4' = e$. Por lo tanto, el grupo alternativo A_4 es resoluble de grado 2, y el grupo simétrico S_4, resoluble de grado 3.

Los grupos resolubles deben su nombre a la teoría de Galois, como se mencionó en el p. 1, § 2 del cap. 1. La resolubilidad del grupo S_4 y de todos sus subgrupos, es causa de la solubilidad en radicales de las ecuaciones algebraicas de grado $n \leqslant 4$. Más detalles sobre estas cuestiones pueden encontrarse en la literatura complementaria, recomendada al principio de la parte I.

3. Grupos simples. Existen grupos $\neq e$ coincidentes con su conmutante y, por lo tanto, insolubles. Más aún, ahora estableceremos la existencia de grupos no abelianos, en los cuales no hay en absoluto subgrupos normales propios ($\neq e$ y G). A estos grupos se adopta llamarlos *simples*.

LEMA. *Cualquier subgrupo normal K del grupo G, es la unión de algún conjunto de clases conjugadas respecto al grupo G.*

Efectivamente, si $x \in K \lhd G$, entonces, $gxg^{-1} \in K$ para todo $g \in G$. En consecuencia, junto con cada elemento $x \in K$, en K está totalmente contenida la clase de elementos conjugados x^G y $K = \bigcup_{i \in I} x_i^{G_i}$. ∎

TEOREMA 5 *El grupo alternativo A_5 es simple.*

DEMOSTRACIÓN. Efectivamente, en el grupo A_5, además de la permutación unitaria e, se tienen 15 elementos $(ij)(kl)$ de orden 2 (de a tres elementos de este tipo en el subgrupo estacionario de cada uno de los puntos 1, 2, 3, 4, 5), $20 = 2\binom{3}{5}$ de elementos (ijk) de orden 3 y $24 = 4!$ del elemento $(1i_1i_2i_3i_4)$ de orden 5. Los elementos de orden 2 son todos conjugados: ellos, evidentemente, están conjugados en S_5, y como el subgrupo estacionario (con relación a la operación por conjugación) del elemento (12) (34) contiene la permutación impar (12), entonces, la conjugación puede ser efectuada mediante permutaciones pares. Lo mismo se refiere a los elementos de orden 3. Pero, los elementos de orden 5, conjugados en S_4, en el grupo A_4 se dividen en dos clases con los representantes (12345) y (12354). En efecto, $(45)(12345)(45)^{-1} = (12354)$, y como centralizador (= subgrupo estacionario) del elemento (12345) en A_5 sirve el grupo cíclico de orden 5, engendrado por este elemento. Así pues, tenemos la tabla

1	15	20	12	12
e	(12) (34)	(123)	(12345)	(12354)

En el renglón inferior se indican los representantes de las clases conjugadas, y en el superior, las potencias de estas clases

Sea ahora K un subgrupo normal respecto a A_5. De acuerdo con el lema

$$|K| = \delta_1 \cdot 1 + \delta_2 \cdot 15 + \delta_3 \cdot 20 + \delta_4 \cdot 12 + \delta \cdot 12.$$

donde $\delta_1 = 1$ (porque $e \in K$) y $\delta_i = 0$ o 1, para $i = 2, 3, 4, 5$. Es fácil convencerse de que la condición de que $|K|$ sea divisor de orden $|A_5| = 60$ (teorema de Lagrange) deja sólo dos posibilidades:

a) $\delta_2 = \delta_3 = \delta_4 = \delta_5 = 0$, K es un subgrupo unidad.

b) $\delta_2 = \delta_3 = \delta_4 = \delta_5 = 1$, $K = A_5$.

Esto demuestra precisamente que A_5 es un grupo simple.

Por inducción sobre n ahora se puede establecer, que *son simples todos los grupos* A_n, $n \geqslant 5$ (resultado de E. Galois) Como los subgrupos de grupos resolubles son también resolubles ($H \subset G \Rightarrow H^{(k)} \subset G^{(k)}$, $k = 1, 2, \ldots$), entonces, del teorema 5, en todo caso, se deduce que el grupo simétrico S_n es insoluble cuando $n \geqslant 5$.

TEOREMA 6 *El grupo de las rotaciones* SO (3) *es simple.*

DEMOSTRACION. De acuerdo con el teorema 3, es suficiente convencerse de que cualquier subgrupo normal K del grupo SU (2), contenedor del núcleo $\{\pm E\}$ del epimorfismo Φ: SU (2) $\to$ SO (3) (véase el p. 3, § 1) y diferente de $\{\pm E\}$, coincide con SU (2). La relación 5 del § 1 puede ser interpretada de otro modo, diciendo, que cada clase conjugada del grupo SU (2) contiene una matriz diagonal $d_\varphi = b_{2\varphi} = \mathrm{diag}\,\{e^{i\varphi}, e^{-i\varphi}\}$. Como, según el lema, K es la unión de alguna familia de clases conjugadas del grupo SU (2), entonces, sin limitación de generalidad, consideramos $d_\varphi \in K$ para algún $\varphi > 0$, tal que sen $\varphi \neq 0$.

En K debe contenerse también cualquier conmutador.

$$[d_\varphi, g] = d_\varphi (g\, d_\varphi^{-1} g^{-1})$$

$$= \begin{Vmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{Vmatrix} \begin{Vmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{Vmatrix} \begin{Vmatrix} e^{-i\varphi} & 0 \\ 0 & e^{i\varphi} \end{Vmatrix} \begin{Vmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{Vmatrix} =$$

$$= \begin{Vmatrix} |\alpha|^2 + |\beta|^2 e^{i2\varphi} & * \\ * & |\alpha|^2 + |\beta|^2 e^{-i2\varphi} \end{Vmatrix},$$

donde $|\alpha|^2 + |\beta|^2 = 1$ (véase (3), § 1). Para la traza de la matriz $[d_\varphi, g]$ obtenemos la expresión

$$\mathrm{tr}\,[d_\varphi, g] = 2|\alpha|^2 + |\beta|^2 (e^{i\varphi 2} + e^{-i2\varphi}) = 2(1 - 2|\beta|^2 \operatorname{sen}^2 \varphi).$$

Aquí, $|\beta|$ toma cualquier valor del intervalo $[0, 1]$ y sen $\varphi \neq 0$. Nuevamente, en virtud de (5) § 1, se hallará la matriz unidad $h \in$ $\in$ SU (2) tal, que $h\,[d_\varphi, g]\,h^{-1} = d_\psi = \mathrm{diag}\,\{e^{i\psi}, e^{-i\psi}\}$, además, $d_\psi \in K$. Como $e^{i\psi}$, $e^{-i\psi}$ son las raíces de la ecuación característica

$$\lambda^2 + (4|\beta|^2 \operatorname{sen}^2 \varphi - 2)\lambda + 1 = 0$$

de la matriz $[d_\varphi, g]$, entonces, haciendo que $|\beta|$ tome los valores de 0 a 1. obtenemos para ψ cualquier punto en el segmento $[0, 2\varphi]$. Y bien, en K está contenido cualquier elemento d_φ y la clase conjugada, definida por el parámetro ψ, cuando $0 \leqslant \psi \leqslant 2\varphi$. Por cuanto para todo $\sigma > 0$ existe un número natural n, que cumple la condición $0 < \psi = \frac{\sigma}{n} \leqslant 2\varphi$, se puede afirmar que en K está contenido el elemento dado de antemano $d_\sigma = d_\psi^n$. ∎

De los teoremas 5 y 6 se aprecia que en la clase de grupos simples se contienen grupos finitos a infinitos de gran importancia práctica. Puede parecer sorprendente que aún no se cuente con una descripción razonable de todos los grupos simples finitos, y no es claro si se puede obtener o no.

4. Productos de grupos. Consideremos ahora una estructura, que permite construir nuevos grupos a partir de otros dados. En distintos casos particulares ya nos hemos encontrado con esta estructura.

Llamemos *producto directo (externo)* de los grupos arbitrarios A y B, al conjunto $A \times B$ de todos los pares ordenados (a, b), donde $a \in A$, $b \in B$, con la operación binaria

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2).$$

Hablando con propiedad, correspondería escribir $(a_1, b_1)*(a_2, b_2) = (a_1 \circ a_2, b_1 \square b_2)$, donde $\circ$, $\square$, $*$, son operaciones binarias en A, B y $A \times B$ respectivamente, pero, para simplificar la escritura, convenimos denotar todas las operaciones con un punto (de paso, omitiéndolo). Para la escritura aditiva de los grupos, por ejemplo, de los abelianos, es natural hablar sobre la suma directa $A \oplus B$.

En $A \times B$ se contienen los subgrupos $A \times e$, $e \times B$, isomorfos a A y B, respectivamente (otra condicionalidad más: los elementos unidades en A y B se anotan con un símbolo e) La aplicación φ: $A \times B \to B \times A$, dada por la igualdad $\varphi((a, b)) = (b, a)$, evidentemente, establece el isomorfismo de los grupos $A \times B$ y $B \times A$. Si tenemos tres grupos A, B, C, entonces, se puede hablar de los productos directos $(A \times B) \times C$ y $A \times (B \times C)$. Haciendo $\psi(((a, b) c)) = (a, (b, c))$, nos convencemos fácilmente de que

$$(A \times B) \times C \quad A \times (B \times C).$$

Las propiedades de conmutatividad y asociatividad del producto directo, nos permiten hablar sobre el producto directo de cualquier número finito de grupos $G_1, G_2, \ldots, G_n$, y escribir

$$G_1 \times G_2 \times \ldots \times G_n = \prod_{i=1}^{n} G_i,$$

sin indicar explícitamente mediante paréntesis, en que orden se toman los productos directos de dos en dos (con esto, transforma-

mos el conjunto de todos los grupos en un semigrupo conmutativo, cuyos elementos son grupos).

TEOREMA 7. *Sea G un grupo con subgrupos normales A y B. Si $A \cap B = e$ y $AB = G$, entonces, $G \cong A \times B$.*

DEMOSTRACION. De la igualdad $AB = G$ se deduce, que cualquier elemento $g \in G$ se escribe en la forma $g = ab$, donde $a \in A$, $b \in B$. Si, además, $g = a_1b_1$, $a_1 \in A$, $b_1 \in B$, entonces, $ab = a_1b_1 \Rightarrow a_1^{-1}a = b_1b^{-1} \in A \cap B = e$. En consecuencia, $a_1 = a$, $b_1 = b$, y llegamos a la conclusión, que la anotación $g = ab$ es unívoca. Luego, $A \lhd G \Rightarrow k = a(ba^{-1}b^{-1}) = aa' \in A$; $B \lhd G \Rightarrow k = (aba^{-1})\, b^{-1} = b'b^{-1} \in B$, o sea, el conmutador $k \in A \cap B = e$ es un elemento unidad y, por lo tanto, $ab = ba$.

Definimos ahora la aplicación $\varphi: G \to A \times B$, haciendo $\varphi(g) = (a, b)$ para cualquier $g = ab$. Conforme a lo antedicho, $\varphi(gg') = \varphi(aba'b') = \varphi(aa'bb') = (aa', bb') = (a, b)(a', b') = \varphi(ab) \times \varphi(a'b') = \varphi(g)\varphi(g')$. Luego, $\varphi(ab) = (e, e) \Leftrightarrow a = e$, $b = e$, o sea, $\operatorname{Ker} \varphi = e$. El epimorfismo de φ es evidente. De este modo, φ satisface todas las propiedades de una aplicación isomorfa de grupos. ∎

El grupo G, que satisface las condiciones del teorema 7, llámase *producto directo* (*interno*) de sus subgrupos A, B. Difiere del producto directo externo en que G contiene en calidad de factores directos los propios grupos A, B, y no sencillamente sus copias isomorfas $A \times e$, $e \times B$. Se sobreentiende, que el producto directo externo $G = A \times B$ también es producto interno de los subgrupos $A \times e$, $e \times B$, y, con cierta experiencia, es posible no hacer diferencias entre ellos, utilizando la expresión reducida «producto directo».

Alguna información sobre los homomorfismos de los productos directos, es dada por el

TEOREMA 8. *Sean, $G = A \times B$, y $A_1 \lhd A$, $B_1 \lhd B$. Entonces, $A_1 \times B_1 \lhd G$ y $G/(A_1 \times B_1) \cong (A/A_1) \times (B/B_1)$. En particular, $G/A \cong B$.*

DEMOSTRACION. Sean, $\pi: A \to A/A_1$ y $\rho: B \to B/B_1$, homomorfismos naturales. Definimos la aplicación $\varphi: G \to (A/A_1 \times (B/B_1)$ por medio de la relación $\varphi(ab) = (\pi(a), \rho(b))$. Se comprueba inmediatamente, que φ es un homomorfismo con núcleo $\operatorname{Ker} \varphi = A_1 \times B_1$ e imagen $(A/A_1) \times (B/B_1)$. ∎

Al igual que en la teoría de los espacios vectoriales, es fácil demostrar que si G es un grupo con subgrupos normales $G_1, \ldots, G_n$, entonces, $G \cong \prod G_i$ sólo en el caso cuando $G = \langle G_1, \ldots, G_n \rangle$ y $G_j \cap \langle G_1, \ldots, \widehat{G_j}, \ldots, G_n \rangle = e$, para todo j (el sombrero $\wedge$ sobre G_j significa que el componente G_j se omitió). Lo mismo se expresa con la propiedad siguiente: *G es el producto directo de sus subgrupos normales $G_1, \ldots, G_n$, ya que cada elemento $g \in G$ permite, además, unívocamente, ser escrito en la forma $g = g_1 \ldots g_n$, $g_i \in G_i$.*

El producto directo de n ejemplares del grupo H también se llama *potencia directa n-ésima* y se anota con el símbolo $H^n = H \times \ldots \times H$. En H^n se destaca un subgrupo especial, la diagonal $\Delta = \{(h, h, \ldots, h) \mid h \in H\}$, isomorfa a H.

Si en el teorema 7 se desprecia la condición $B \triangleleft G$, entonces, llegaremos al concepto de *producto semidirecto*: $G = AB$, $A \cap B = e$, $A \triangleleft G$ (a veces se escribe $G = A \times B$). En esta definición correspondería introducir también la descripción de la operación del subgrupo B con los automorfismos en el subgrupo normal A, lo que ordinariamente se hace en cada caso concreto.

Muchos de los grupos que conocemos, se representan en forma de productos directos y semidirectos. Por ejemplo, S_n es el producto semidirecto del subgrupo normal A_n por el grupo cíclico $\langle(12)\rangle$ de orden 2: $S_n \cong A_n \times Z_2$. Utilizando las anotaciones del ejemplo 2, p. 1, se puede escribir: $A_4 = V_4 \times \langle(123)\rangle \cong (Z_2 \times Z_2) \times Z_3$; $S_4 = V_4 \times S_3 \cong (Z_2 \times Z_2) \times (Z_3 \times Z_2)$. Otro ejemplo más: el grupo $A(1, \mathbb{R})$ de las transformaciones afines $\mathbb{R} \to \mathbb{R}$ (véase el ejercicio 3, § 2, cap. 4) es un producto semidirecto de un subgrupo normal de traslaciones por el subgrupo $GL(1, \mathbb{R})$ de ransformaciones, que dejan el punto $x = 0$ en su lugar.

5. Generadores y relaciones determinates. La cuestión sobre los sistemas de generadores del grupo G ya se discutío en el § 2 del cap. 4. Regresamos a ella para echar una mirada a algunos grupos que conocemos, desde un nuevo punto de vista. De los resultados del cap. 4 se deduce que para los grupos cíclicos no hay necesidad de componer las enormes tablas de Cayley. La escritura condicional

$$C_n = \langle c \mid c^n = e \rangle \tag{3}$$

brinda toda la información necesaria sobre el grupo cíclico abstracto C_n, de orden n, se supone, que $C_n = \{e, c, c^2, \ldots, c^{n-1}\}$, además. $c^s c^t = c^{s+t}$ para $s + t < n$, y $c^s c^t = c^{s+t-n}$ cuando $s + t \geqslant n$, Por otra parte, todo grupo cíclico es, con exactitud hasta el isomorfismo, una imagen homomorfa de un grupo único $(\mathbb{Z}, +)$.

En este sentido, como grupo universal para todos los productos directos posibles $A = \langle a_1 \rangle \times \ldots \times \langle a_r \rangle$ de los grupos cíclicos de órdenes $n_1, \ldots, n_r$ (n_i es un número natural o el símbolo ∞) serviá la r-ésima potencia directa $\mathbb{Z}^r = \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ (véase el p. 4) con los generadores

$$z_i = (0, \ldots, 1, \ldots, 0), \quad i = 1, 2, \ldots, r,$$

y la composición

$$\sum s_i z_i + \sum t_i z_i = \sum (s_i + t_i) z_i = (s_1 + t_1, \ldots, s_r + t_r).$$

La aplicación $z_i \mapsto a_i$, $1 \leqslant i \leqslant r$, se continúa unívocamente hasta el homomorfismo de los grupos φ: $(s_1, s_2, \ldots, s_r) \to a_1^{s_1} a_2^{s_2} \ldots a_r^{s_r}$

con núcleo $\operatorname{Ker}\varphi = m_1\mathbb{Z} \oplus \ldots \oplus m_r\mathbb{Z}$ (véase el teorema 8), donde $m_i = n_i$, si $n_i < \infty$, y $m_i = 0$, si $n_i = \infty$.

Por analogía con (3), se puede escribir

$$A = \langle a_1, \ldots, a_r \mid a_1^{m_1} = e, \ldots, a_r^{m_r} = e \rangle,$$

suponiendo tácitamente, que los generadores $a_1, \ldots, a_r$, además, conmutan. Las expresiones $a_1^{m_1} = e, \ldots, a_r^{m_r} = e$ se denominan *relaciones determinantes* del grupo abeliano A, y $\mathbb{Z}^r$ se llama *grupo abeliano libre de rango r* (*o con r generadores libres* $z_1, \ldots, z_r$). Es evidente, que

$$A \cong \mathbb{Z}^r \Leftrightarrow (a_1^{s_1} \ldots a_r^{s_r} = e \Leftrightarrow s_1 = \ldots = s_r = 0).$$

Si ahora, F_d es un grupo arbitrario, engendrado por d generadores $f_1, \ldots, f_d$, entonces, cada uno de sus elementos f, se escribe (posiblemente, de muchos modos) en la forma

$$f = f_{i_1}^{s_1} f_{i_2}^{s_2} \ldots f_{i_k}^{s_k}; \quad i_j \in \{1, 2, \ldots, d\}, \quad s_j \in \mathbb{Z}, \tag{4}$$

donde $i_j \neq i_{j+1}$, $j = 1, 2, \ldots, k-1$. Esto siempre se consigue con las sustituciones elementales $f_i^s f_i^t = f_i^{s+t}$, $f_i = e$ y $f_j e = e f_j = f_j$.

Cuando se cumple la condición $f = e \Leftrightarrow s_1 = \ldots = s_k = 0$ para cada f, anotada en la forma (4), se dice, que *F_d es un grupo libre, engendrado por d generadores libres*. Los elementos del grupo F_d habitualmente se llaman *palabras en el alfabeto* $\{f_1, f_1^{-1}, \ldots, f_d, f_d^{-1}\}$. *La escritura irreducible* (4) *de la palabra f* y su *longitud* $l(f) = |s_1| + |s_2| + \ldots + |s_k|$ están definidas unívocamente: en caso contrario, la palabra vacía $e = ff^{-1}$ (elemento unidad en F_d) tendría una longitud >0. Para un d dado, dos grupos libres F_d y G_d, engendrados por los generadores libres $f_1, \ldots, f_d$ y $g_1, \ldots, g_d$, respectivamente, son isomorfos: es suficiente hacer $\Phi(f_i) = g_i$, $1 \leqslant i \leqslant d$, y para la palabra arbitraria f de la forma (4) contar

$$\Phi(f) = g_{i_1}^{s_1} g_{i_2}^{s_2} \ldots g_{i_k}^{s_k}$$

(las unidades, en F_d y G_d tienen el mismo símbolo). Si, no obstante, G_d no es un grupo libre, entonces, Φ será sólo un epimorfismo con núcleo $\operatorname{Ker}\Phi$ compuesto de aquellas palabras que con la sustitución $f_i \mapsto g_i$ pasan al elemento unidad del grupo G_d. Esta *propiedad universal* (posibilidad de continuar $f_i \to g_i$, $1 \leqslant i \leqslant d$, hasta el epimorfismo Φ: $F_d \to G_d$ para cualquier grupo C_d con d generadores) se puede tomar como definición del grupo libre F_d, pero no nos detendremos en esto.

Para que los grupos libres no parezcan objetos místicos, ofrecemos algunas de sus realizaciones concretas.

$d = 1$. $F_1 \cong (\mathbb{Z}, +)$ es el grupo libre abeliano de rango 1, o, lo que es igual, el grupo cíclico infinito.

$d = 2$. Sea $\mathbb{Z}[t]$ el anillo de los polinomios en t con coeficientes racionales enteros. En el grupo lineal especial SL $(2, \mathbb{Z}[t])$ examinemos el subgrupo F, engendrado por las matrices

$$A = \begin{Vmatrix} 1 & t \\ 0 & 1 \end{Vmatrix}, \quad B = \begin{Vmatrix} 1 & 0 \\ t & 1 \end{Vmatrix}.$$

Demostremos, que F es un grupo libre. Una inducción liviana sobre k muestra, que el elemento

$$W_k = A^{\alpha_1}B^{\beta_1} \ldots A^{\alpha_k}B^{\beta_k}, \quad \alpha_i,\ \beta_i \neq 0, \quad 1 \leqslant i \leqslant k,$$

tiene la forma

$$W_k = \begin{Vmatrix} 1 + \ldots + \sigma^k t^{2k} & t(\ldots + \sigma_{k-1}\alpha_k t^{2(k-1)}) \\ t(\ldots - \alpha_1^{-1}\sigma_k t^{2(k-1)}) & 1 + \ldots + \alpha_1^{-1}\sigma_{k-1}\alpha_k t^{2(k-1)} \end{Vmatrix},$$

donde $\sigma_k = \alpha_1\beta_1 \ldots \alpha_k\beta_k$, y con puntos se indican los monomios de menor potencia con respecto a t. Es claro, que $W_k \neq E$. Cualquier elemento del grupo F se escribe bien en la forma $B^\beta A^\alpha \neq E$, o bien en la forma $W = B^\beta W_k A^\alpha$. Si $W = E$, entonces, $W_k = B^{-\beta}A^{-\alpha}$, lo que, sin embargo, es imposible (comparar las potencias para $k > 1$, y $k = 1$ y efectuar la comprobación inmediata).

Un sencillo razonamiento complementario muestra, que con la sustitución $t = m$, donde m es un número entero cualquiera $\geqslant 2$, el grupo F continúa siendo libre.

Ahora, introducimos la siguiente

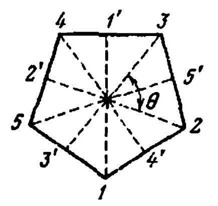
DEFINICION. Sea, F_d un grupo libre con d generadores libres $f_1, \ldots, f_d$; $S = \{w_i,\ i \in I\}$, algún subconjunto de los elementos $w_i\ (f_1, \ldots, f_d) \in F_d$, y $K = \langle S^{F_d}\rangle$ el menor subgrupo normal en F_d, contenedor de S (intersección de todos los subgrupos normales, contenedores de S). Se dice que *el grupo G está dado por d generadores $a_1, \ldots, a_d$ y por las relaciones $w_i\ (a_1, \ldots, a_r) = e$*, $i \in I$, si existe el epimorfismo $\pi\colon F_d \to G$ con núcleo K tal, que $\pi(f_k) = a_k$, $1 \leqslant k \leqslant d$. Además, se escribe

$$G = \langle a_1, \ldots, a_d \mid w_i\ (a_1, \ldots, a_d) = e, \quad i \in I\rangle$$

y llaman a G *grupo finitamente determinado*, ya que Card $I < \infty$. El propio grupo F_d está «libre de relaciones», lo que explica su nombre. De la definición se deduce que cualpuier grupo H con d generadores $b_1, \ldots, b_d$, que satisfacen las mismas relaciones $w_i\ (b_1, \ldots, b_d) = e$, $i \in I$, y, posiblemente, algunas otras, es la imagen homomorfa del grupo G. En particular, $|H| \leqslant |G|$.

EJEMPLO 1. (*grupo de diedro*). El grupo $G = \langle a, b^2 \mid a^3 = b^2 = abab = e\rangle$ con dos generadores y tres relaciones, tiene el orden $|G| \leqslant 6$, por cuanto $ba = a^{-1}b^{-1} = (a^3)^{-1}\cdot a^2b\cdot(b^2)^{-1} = a^2b$ y G, en todo caso, se agota con lo elementos e, a, a^2, b, ab, a^2b. Como, para las permutaciones (123), (12), generadoras de S_3, se cumplen las relaciones $(123)^3 = (12)^2 = (123)\ (12)\ (123)\ (12) = e$,

entonces, la aplicación $\varphi: G \to S_3$ definida por la correspondencia $a \to (123)$, $b \to (12)$, será el isomorfismo $G \cong S_3$. Por lo tanto, el grupo simétrico S_3 es dado por dos generadores y tres relaciones. Recordemos que S_3 también se



identifica con el grupo de todas las transformaciones de simetría del triángulo equilátero.

El grupo completo de transformaciones de simetría del n-ágono regular P_n se llama *grupo del diedro* (*grupo diedral*) y se anota con el símbolo D_n. La rotación

$$\mathcal{A} = \left\| \begin{matrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{matrix} \right\|$$

de un polígono en su superficie a un ángulo $\theta = 2\pi/n$ alrededor del centro O, ubicado en el origen del sistema de coordenadas cartesianas, engendra el grupo cíclico $\langle \mathcal{A} \rangle$ de orden n. En D_n está contenida también la reflexión $\mathcal{B} = \left\| \begin{matrix} 1 & 0 \\ 0 & -1 \end{matrix} \right\|$ del polígono P_n en relación con el eje que pasa por el centro y uno de sus vértices.

Por definición, $\mathcal{B}^2 = e$. Las distintas transformaciones de simetría

$$e, \mathcal{A}, \mathcal{A}^2, \ldots, \mathcal{A}^{n-1}; \quad \mathcal{B}, \mathcal{A}\mathcal{B}, \ldots, \mathcal{A}^{n-1}\mathcal{B} \tag{5}$$

en la cantidad $2n$, agotan el grupo D_n. Efectivamente, toda transformación de simetría se define por su operación en los vértices $1, 2, \ldots, n$ del polígono P_n. Si alguna transformación traslada 1 a k, entonces, o debe conservar el mismo orden cíclico de vértices, como lo hace $\mathcal{A}^k$, o bien cambiarlo por el inverso, como lo hace $\mathcal{A}^{k-1}\mathcal{B}$. Por eso, ningún otro elemento, excepto (5), en D_n no hay. Observemos, que la transformación $\mathcal{B}\mathcal{A}$ coincide con $\mathcal{A}^{n-1}\mathcal{B}$, por cuanto ambas giran el orden de los vértices y trasladan 1 a n. De este modo, tienen lugar las relaciones

$$\mathcal{A}^n = e, \quad \mathcal{B}^2 = e, \quad \mathcal{A}\mathcal{B}\mathcal{A}\mathcal{B} = e.$$

Esto significa, que D_n es imagen homomorfa del grupo

$$G = \langle a, b \mid a^n = b^2 = abab = e \rangle.$$

Pero, como cuando $n = 3$, obtenemos $ba = a^{-1}b = a^{n-1}$, así que cualquier palabra en el alfabeto $\{a, a^{-1}, b, b^{-1}\}$ se reduce a a^i, o bien a $a^i b$, $0 \leqslant i \leqslant n-1$. Por lo tanto, $|G| \leqslant 2n$, y en virtud de lo dicho anteriomente, deberá tener lugar el isomorfismo $G \cong D_n$. De este modo, el grupo diedral ha sido dado mediante los generadores y relaciones determinantes. Identifiquemos G con D_n:

$$D_n = \langle a, b \mid a^n = e, \quad b^2 = e, \quad (ab)^2 = e \rangle.$$

Como $\langle a \rangle \lhd D_n$ y $D_n/\langle a \rangle$ es un grupo cíclico, entonces, en base al teorema 4 para el conmutante D_n' del grupo D_n, tenemos la inclusión $D_a' \subset \langle a \rangle$. Pero, $a^2 = aba^{-1}b^{-1} = [a, b] \in D_n'$; cuando n es impar $D_n' = \langle a \rangle$, y cuando n es par $D_n/\langle a^2 \rangle = \langle \bar{a}, \bar{b} \rangle \cong V_4$ es el producto directo de dos grupos cíclicos de

orden 2, de donde $D'_n = \langle a^2 \rangle$. De acuerdo a la paridad de n, también varía el centro $Z(D_n)$ del grupo D_n y el número r de sus clases conjugadas.

Mostramos las tablas preparadas (y fácilmente comprobables):

$$n = 2m, \quad D'_n = \langle a^2 \rangle, \quad (D_n : D'_n) = 4, \quad Z(D_n) = \langle a^m \rangle, \quad r = m + 3$$

1	1	2	...	2	m	m
e	a^m	a	...	a^{m-1}	b	ab

$$n = 2m + 1, \quad D'_n = \langle a \rangle, \quad (D_n : D'_n) = 2, \quad Z(D_n) = e, \quad r = m + 2$$

1	2		2	2	n
e	a	...	a^{m-1}	a^m	b

Los representantes de las clases conjugadas están en la fila inferior y las potencias de estas clases, en la superior.

Queda por subrayar, que la forma de las relaciones determinantes (sus primeros miembros en la escritura $w_i = e$) depende esencialmente de la elección del sistema de los grupos generadores. Por ejemplo,

$$D_n \langle g_1, g_2 \mid g_1^2 = g_2^2 = (g_1 g_2)^n = e \rangle.$$

Si se parte de la tarea anterior, se puede hacer $g_1 = ab$, $g_2 = b$.

EJEMPLO 2. (*grupo de cuaterniones*). A diferencia del ejemplo anterior, desde un principio definimos el grupo de cuaterniones Q_8 (el nombre se explica en el cap. 9) por sus generadores y relaciones:

$$Q_8 = \langle a, b \mid a^4 = e, \quad b^2 = a^2, \quad bab^{-1} = a^{-1} \rangle.$$

Nuevamente, $ba = a^{-1}b = a^3b$ y, por cuanto $b^2 = a^2$, cualquier palabra en el alfabeto $\{a, a^{-1}, b, b^{-1}\}$ se lleva a la forma a^sb^t, $0 \leqslant s \leqslant 3$, $0 \leqslant t \leqslant 1$, por lo tanto $|Q_8| \leqslant 8$.

¿Podemos afirmar que $|Q_8| = 8$? Sí, pero sólo después de que haya sido presentado un grupo de 8 elementos, con dos generadores del mismo vinculados por las mismas relaciones que a, b. Un grupo así es engendrado por las matrices

$$A = \begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix}, \quad B = \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix} \quad (i = \sqrt{-1}),$$

En efecto,

$$A^4 = E, \quad B^2 = A^2, \quad BAB^{-1} = A^{-1}$$

$$\text{y } \langle A, B \rangle = \left\{ \pm \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \pm \begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix}, \pm \begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}, \pm \begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix} \right\}.$$

La aplicación $a \to A$, $b \to B$ define el isomorfismo $Q_8 \cong \langle A, B \rangle$. Observemos que $a^2 \in Z(Q_8)$, y como el grupo cociente respecto al centro de un grupo no abeliano no puede ser cíclico (véase la observación en el p. 2), entonces, $\langle a^2 \rangle = Z(Q_8)$. Todos los grupos de orden 4 son abelianos, por eso $Q_8/Z(Q_8) \cong \cong V_4$, es el producto directo de dos grupos cíclicos de orden 2. Por lo tanto el conmutante Q'_8 coincide con $Z(Q_8)$ y $(Q_8 : Q'_8) = 4$. Los datos sobre clases

conjugadas, se tienen en la tabla:

1	1	2	2	2
e	a^2	a	b	ab

Los grupos finitamente determinados, de los que examinamos ejemplos elementales, se encuentran en diversos dominios de las matemáticas, por ejemplo, en calidad de los llamados grupos fundamentales de heterogeneidades. No sorprende, que muchas cuestiones referidas a ellos, no han sido resueltas.

EJERCICIOS

1. Recordemos la definición del p. 2, § 3, cap. 4, de automorfismo interno I_a: $g \to aga^{-1}$ y de grupo Inn $(G) \subset$ Aut (G). Mostrar, que Inn $(G) \lhd$ Aut (G) y Inn $(G) \cong G/Z(G)$, donde $Z(G)$ es el centro del grupo G. El grupo cociente Out (G) = Aut (G)/Inn(G) se llama *grupo de automorfismos externos*.

2. Sean H y K, subgrupos del grupo G. Mostrar, que $|HK| \times |H \cap K| = |H| \cdot |K|$ análogo de la fórmula conocida de la teoría de espacios lineales). Mostra, a continuación que el conjunto HK será subgrupo si, y sólo si, $HK = KH$, cuando $K \lhd G$, esta condición se cumple automáticamente.

3. Mostrar que en el grupo resoluble finito G, se hallará una sucesión de subgrupos $e = G_0 \subset G_1 \subset \ldots \subset G_n = G$, donde $G_{i-1} \lhd G_i$, $1 \leqslant i \leqslant n$, y cada índice $(G_i : G_{i-1}) = p_i$ es algún número primo.

4. Componer para el grupo simétrico S la tabla

1	3	6	8	6
e	(12) (34)	(12)	(123)	(1234)

análoga a la que usamos en el curso de la demostración del teorema 5. Apoyándose en los mismos razonamientos, repetir la discripción de los subgrupos normales del grupo S_4, que hemos dado en el ejemplo 2.

5. Demostrar que el grupo alternativo A_n, $n \geqslant 5$ es simple, observando el esquema de razonamientos expuesto a continuación.

a) En el subgrupo normal $K \lhd A_n$, $K \neq e$, corresponde tomar la permutación $\pi \neq e$, que deje en su lugar el mayor número k posible de símbolos de $\Omega = \{1, 2, \ldots, n\}$. Si $k = n - 3$, entonces, $\pi = (ijk)$ y $K = A_n$ (véase el ejercicio 8, § 2 del cap. 4), por eso, consideramos $k < n - 3$.

b) Si $\pi = (123\ \ldots)$ es el desarrollo de π en ciclos independientes, entonces la paridad de π y la condición $k < n - 3$ conllevan $k \leqslant n - 5$. También es posible, que $\pi = (12)(34) \ldots$ se componga de ciclos independientes de longitud 2.

c) En todo caso, examinar el conmutador $[\pi, \sigma] = \pi\sigma\pi^{-1}\sigma^{-1} \neq e$ con $\sigma = (345)$ y comprobar que él deja en su lugar más de k símbolos. Esto contradice la elección de k y demuestra la afirmación.

6. Mostrar, que $Z(A \times B) = Z(A) \times Z(B)$.

7. Si $K_1, K_2 \lhd G$, $K_1 \cap K_2 = e$, entonces, G es isomorfo a un cierto subgrupo en $(G/K_1) \times (G/K_2)$. ¿Es cierto ésto?

8. Sea $K \lhd G = A \times B$. Demostrar que, bien el subgrupo K es abeliano, bien una de las intersecciones $K \cap A$, $K \cap B$ es no trivial. Dar un ejemplo de grupo $A \times B$ con subgrupo normal no trivial K tal, que $K \cap A = e$ y $K \cap \cap B = e$. Con esto, de $K \lhd A \times B$, hablando en general, no se deduce que $K = (K \cap A) \times (K \cap B)$.

9. ¿Es o no el grupo de cuaterniones Q_8 producto semidirecto de algunos de sus dos propios subgrupos?

10. Mostrar que $H \lhd Q_8$ para cualquier subgrupo propio $H \subset Q_8$.

11. Mostrar, que los grupos D_4 y Q_8 no son isomorfos. (*Indicación.* Contar los elementos de orden 2 o utilizar el resultado del ejercicio 10.)

12. Mostrar que $\mathrm{Aut}(D_4) \cong D_4$ (como $|Z(D_4)| = 2$, entonces, de acuerdo con la afirmación 1, $\mathrm{Out}(G) = 2$).

13. Todas las raíces complejas de primer grado p^i, $i = 0, 1, 2, \ldots$, forman el grupo infinito $C(p^\infty)$. El se llama cuasicíclico, por cuanto cualquier número finito de sus elementos engendra un grupo cíclico. Comprobar esto y mostrar que

$$C(p^\infty) = \langle a_1, a_2, a_3, \ldots \mid a_1^p = 1, \quad a_{i+1}^p = a_i, \quad i = 1, 2, 3, \ldots \rangle.$$

14. (J. Monthly 80, N° 9 (1973).) Sea

$$G = \langle a, b \mid aba = ba^2b, \quad a^3 = e, \quad b^{2n-1} = e \rangle,$$

donde $n \in \mathbb{N}$. Demostrar que $n = 1$, o sea, $b = e$ y, de hecho, $G = \langle a \mid a^3 = e \rangle$ es un grupo cíclico de orden 3. (*Indicación.* $aba = ba^2b = ba^{-1}b \Longrightarrow ab^2 = aba \cdot a^{-1}b = ba^{-1}b \cdot a^{-1}b = ba^{-1} \cdot aba = b^2a$. Sacar de aquí la conclusión de que $ab = ba$ y, en consecuencia, teniendo en cuenta otras relaciones, $b = e$)

15. Completar con detalles la definición formal siguiente de grupo libre F_n con n generadores. Al alfabeto $A = \{a_1, a_1^{-1}, \ldots, a_n, a_n^{-1}\}$, compuesto de n letras $a_1, \ldots, a_n$ y sus «antípodas» $a_1^{-1}, \ldots, a_n^{-1}$, se lo agrega el símbolo e. Sea S el conjunto de todas las «palabras» obtenidas mediante la escritura de estos $2n + 1$ símbolos en cualquier orden, en filas de longitud finita. Se permite repetir símbolos en las palabras. Por producto uv de dos palabras u, v, se entiende la agregación de la palabra v al final de la u. Se llama inversa a $u = a_{i_1}^{\varepsilon_1} \ldots a_{i_m}^{\varepsilon_m}$, $\varepsilon_k = \pm 1$, $k = 1, \ldots, m$, la palabra $u^{-1} = a_{i_m}^{-\varepsilon_m} \ldots a_{i_1}^{-\varepsilon_1}$, $e^{-1} = e$. En S se introduce la relación de equivalencia. Precisamente, dos palabras se consideran equivalentes si una se obtiene de otra como resultado del empleo de un número finito de las transformaciones elementales siguientes:

$$ee \sim e,$$
$$a_ia_i^{-1} \sim e, \quad a_i^{-1}a_i \sim e,$$
$$a_ie \sim a_i, \quad a_i^{-1}e \sim a_i^{-1},$$
$$ea_i \sim a_i, \quad ea_i^{-1} \sim a_i^{-1}.$$

En cada clase de equivalencia hay una única palabra «no simplificable» (más corta). En las clases de equivalencia respecto a la relación está definida la operación asociativa de multiplicación (y rotación de clases), inducida por la multiplicación de palabras. Será unidad la clase de equivalencia de la palabra «vacía» e. El conjunto de clases de equivalencia, con la operación de multiplicación dada, es, precisamente, el grupo libre F_n con n generadores $a_1, \ldots, a_n$ (grupo libre de rango n).

EJEMPLO. Por «el ocho», que encierra en sus ojales dos columnas, corre en distintas direcciones un niño con un ovillo, colocando cada vuelta siguiente

sobre las anteriores. Los caminos recorridos por él con puntos iniciales y finales en el centro entre las columnas se interpretan, evidentemente, como elementos del grupo libre F_2 de rango 2. Las palabras no simplificables corresponden a los hilos tirantes, liberados de los ojales triviales aa^{-1}, $a^{-1}a$, bb^{-1}, $b^{-1}b$. En la

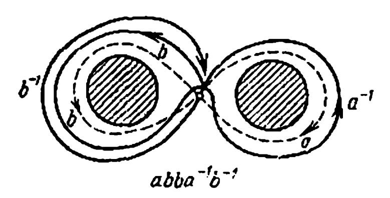


Fig. 20

fig. 20, las partes a y a^{-1}, b y b^{-1}, están representadas geométricamente distintas, sólo para facilitar la comprensión. Nuestro ejemplo realiza F_2 en forma de un conjunto de clases de «caminos homotópicamente equivalentes» (terminología topológica) de lemniscata. En este sentido, el grupo fundamental do pétalo, representado en la fig. 21 (pág. 333) será el grupo libre F_5.

§ 4. TEOREMAS DE SILOV

En el punto 4, § 3, cap. 5 prestamos atención al hecho de que en el grupo finito G de orden $|G|$ puede no haber ningún subgrupo de orden d, divisor de $|G|$. De ejemplo mínimo, sirve el par $G = A_4$, $d = 6$.

Como en un grupo simple no abeliano no puede haber subgrupos de índice 2 (en virtud de su normalidad), entonces, según el teorema 5 del § 3, en el grupo alternativo A_5 de orden 60 no hay subgrupos de orden 30. En efecto, en A_5 tampoco hay subgrupos de órdenes 20 y 15. (¿Por qué?) Use los razonamientos expuestos en el ejemplo 2, p. 3, § 2). Sobre este fondo, especialmente notables parecen las leyes generales, que hace más de un siglo formuló el matemático noruego Sílov. Ellas se refieren a los p-grupos (con los cuales nos encontramos en el § 2), contenidos en calidad de subgrupos del grupo G. La existencia del elemento de orden p en el grupo abeliano, cuyo orden se divide por p, fue observado ya por O. Cauchy.

Sea $|G| = p^n m$, donde p es un número primo y m uno entero, además, p y m son primos entre sí. Al subgrupo $P \subset G$ de orden $|P| = p^n$ (si existe) lo llamaremos *p-subgrupo de Sílov* del grupo G. Como en el p. 3 del § 2, por $N(P)$ se comprende el normalizador del subgrupo P en G.

TEOREMA 1. (primer teorema de Sílov). *Los p-subgrupos de Sílov, existen.*

TEOREMA 2. (segundo teorema de Sílov). *Sean P y P_1 dos p-subgrupos de Sílov cualesquiera del grupo G.* Entonces, *existirá un elemento*

$a \in G$, para el cual $P_1 = aPa^{-1}$. *Con otras palabras, todos los p-subgrupos de Sílov están conjugados.*

TEOREMA 3 (tercer teorema de Sílov). *Para el número N_p de los p-subgrupos de Sílov del grupo G, tiene lugar la igualdad $N_p = (G: N(P))$ y la congruencia $N_p \equiv 1 \pmod p$.*

Las demostraciones de los teoremas 1 — 3, sirven de ilustración de los métodos generales y razonamientos expuestos en el § 2. Comenzamos con el teorema 2.

DEMOSTRACION del teorema 2. Y bien, sea que los p-subgrupos de Sílov en G existen, y P es uno de ellos. Sea, luego, P_1 un p-subgrupo arbitrario del grupo G, no necesariamente de Sílov. Obligamos a P_1 a operar con traslaciones por la izquierda en el conjunto $G/P = \bigcup_i g_iP$ de clases adjuntas por la izquierda de G respecto a P (la limitación de la operación de G en G/P descrita en el § 2). De acuerdo con los resultados del p. 2, § 2, la longitud de cualquier órbita con relación a P_1, divide el orden $|P_1| = p^k$, $k \geqslant n$. De este modo,

$$m = \frac{p^n m}{p^n} = \frac{|G|}{|P|} = |G/P| = p^{k_1} + p^{k_2} + \ldots,$$

donde $p^{k_1}, p^{k_2}, \ldots$ son las longitudes de las órbitas. Como el m.c.d. $(m, p) = 1$, entonces, por lo menos una órbita tiene la longitud $p^{k_i} = 1$, o sea,

$$P_1 \cdot aP = aP \tag{1}$$

para algún elemento $a = g_i \in G$ (esto se parece a la demostración del teorema 2, § 2). Reescribimos la relación (1) en la forma

$$P_1 \cdot aPa^{-1} = aPa^{-1},$$

llegamos a la conclusión, que

$$P_1 \subset aPa^{-1} \tag{2}$$

(por cuanto aPa^{-1} es un grupo). En particular, si P_1 es un p-subgrupo de Sílov, entonces, $|P_1| = |P|$ y de (2) se deduce que $P_1 = aPa^{-1}$.

DEMOSTRACION de los teoremas 1 y 3. El teorema 1 se puede interpretar como corolario del teorema 3, puesto que $N_p \equiv 1 \pmod p) \Rightarrow N_p \neq 0$, y $N_p \neq 0 \Leftrightarrow S \neq \varnothing$, S es el conjunto de todos los p-subgrupos de Sílov del grupo G.

En lo que respecta al teorema 3, la igualdad $N_p = (G: N(P))$ se deduce directamente de la conjugación de los p-subgrupos de Sílov (teorema 2) y de la afirmación general sobre la longitud de la órbita H^G en el § 2. A la congruencia $N_p \equiv 1 \pmod p$ llegaremos examinando una situación un poco más general. Precisamente, sea $|G| = p^s t$, donde $s \leqslant n$ (t puede dividirse por p), y sea $N_p(s)$ *el número de todos los subgrupos de orden p^s en G. Resulta que tiene lugar la congruencia* $N_p(s) \equiv 1 \pmod p$; en particular G contiene subgrupos de cualquier orden p^s, $s = 1, 2, \ldots, n$ y $N_p(n) = N_p$.

Razonamos del modo siguiente. La operación con traslaciones por la izquierda del grupo G en sí mismo induce, conforme a la observación al final del p. 1, § 2, la operación de G en el conjunto

$$\Omega = \{M \subset G \mid |M| = p^s\}$$

de todos los subconjuntos $\{g_1, \ldots, g_{p^s}\}$ de p^s elementos cada uno. Recordemos que $g \cdot \{g_1, \ldots, g_{p^s}\} = \{gg_1, \ldots, gg_{p^s}\}$. El conjunto Ω se parte en G-órbitas Ω_i: $\Omega = \bigcup \Omega_i$, de modo que

$$|\Omega| = \sum_i |\Omega_i|, \quad |\Omega_i| = (G : G_i),$$

donde $G_i = \{g \in G \mid gM_i = M_i\}$ es subgrupo estacionario de algún representante $M_i \in \Omega_i$.

Como $G_iM_i = M_i$, entonces, $M_i = \bigcup_{j=1}^{\nu_i} G_ig_{ij}$ es la unión de varias clases adjuntas por la derecha de G con relación a G_i. Por eso, $p^s = |M_i| = \nu_i |G_i|$, de donde, $|G_i| = p^{s_i} \leqslant p^s$. En el caso en que $|G_i| < p^s$, tenemos $|\Omega_i| = p^{s-s_i}t \equiv 0 \pmod{pt}$; las igualdades $|G_i| = p^s$ y $|\Omega_i| = t$ son equivalentes. Obtenemos

$$\binom{|G|}{p^s} = |\Omega| \equiv \sum_{|\Omega_i|=t} |\Omega_i| \pmod{pt}. \tag{3}$$

Conforme a lo expresado anteriormente, $|\Omega_i| = t \Rightarrow |G_i| = p^s \Rightarrow M_i = G_ia_i$ ($a_i = g_{i1}$ es algún elemento de G) y, por lo tanto, $a_i^{-1}M_i = a_i^{-1}G_ia_i = P_i$ es un subgrupo de orden p^s). La órbita Ω_i se agota con algún número de clases adjuntas por la izquierda P_i del grupo G respecto a P_i.

Recíprocamente, cada subgrupo $H \subset G$ de orden $|H| = p^s$, lleva a la órbita $\Omega' = \{gH \mid g \in G\}$ de longitud t. Los distintos subgrupos H_i con $|H_i| = p^s$ conllevan a distintas órbitas Ω_i', por cuanto, de $H_i = gH_j$, sigue $e = gh_j$, de donde $g = h_j^{-1} \in H_j$ y $H_i = H_j$. De esta manera, se tiene una correspondencia biunívoca entre los subgrupos de orden p^s y las órbitas Ω_i de longitud t. La congruencia (3) se reescribe en la forma

$$\binom{|G|}{p^s} \equiv \sum_{|\Omega_i|=t} |\Omega_i| \equiv tN_p(s) \pmod{(pt)}, \tag{4}$$

donde correspondería escribir $N_p(s, G)$, a fin de subrayar la dependencia de $N_p(s)$ respecto a G.

Hasta ahora, la especificidad del grupo G no desempeñó ningún papel. Si se toma G como un grupo cíclico de orden p^st, entonces, para él, $N_p(s, G) = 1$ (teorema 5, § 3, cap. 4), y, por eso

$$\binom{|G|}{p^s} \equiv t \cdot 1 \pmod{pt}. \tag{5}$$

Como los primeros miembros de las congruencias (4) y (5) respecto a un mismo módulo pt coinciden, entonces, tenemos

$$t \equiv tN_p(s) \pmod{pt},$$

que brinda precisamente la congruencia buscada $N_p(s) \equiv 1 \pmod p$. ■

Aunque en realidad se ha demostrado más de lo que se pedía, no nos disponemos utilizar este hecho, recomendando a los interesados la literatura especial.

EJEMPLO. Sea $G = SL(2, Z_p)$ el grupo de todas las matrices de dimensiones 2×2, con determinante 1, sobre el campo Z_p de p elementos. De la descomposición

$$GL(2, Z_p) = \bigcup_{i=1}^{p-1} \begin{Vmatrix} i & 0 \\ 0 & 1 \end{Vmatrix} SL(2, Z_p)$$

del grupo lineal completo $GL(2, Z_p)$ en las clases adjuntas respecto a $SL(2, Z_p)$ se deduce que

$$|GL(2, Z_p)| = (p-1)\,|SL(2, Z_p)|. \tag{6}$$

Examinando $GL(2, Z_p)$ como grupo de automorfismos del espacio vectorial bidimensional V sobre Z_p, es fácil hallar el orden de $|GL(2, Z_p)|$. Efectivamente, $GL(2, Z_p)$ opera en el conjunto de pares $\{v_1, v_2\}$ de los vectores básicos. Cualquier vector $f_1 \in V$ diferente de cero (en total hay $p^2 - 1$ unidades) puede ser imagen de v_1, y, sea cual sea la elección de f_1, imagen de v_2 puede ser un vector arbitrario f_2 de $V \setminus \langle f_1 \rangle$ (de ellos se tienen $p^2 - p$ unidades). Por lo tanto, $|GL(2, Z_p)| = (p^2-1)(p^2-p)$, que en combinación con (6) conduce a la fórmula

$$|SL(2, Z_p)| = p(p^2-1).$$

Por lo menos dos p-subgrupos de Silov del grupo $SL(2, Z_p)$ hallamos enseguida:

$$P_1 = \left\{ \begin{Vmatrix} 1 & \alpha \\ 0 & 1 \end{Vmatrix} \,\middle|\, \alpha \in Z_p \right\}, \quad P_2 = \left\{ \begin{Vmatrix} 1 & 0 \\ \alpha & 1 \end{Vmatrix} \,\middle|\, \alpha \in Z_p \right\}.$$

En correspondencia con el teorema 3 tenemos

$$n_p = (G : N(p)) = 1 + kp > 1,$$

y como

$$\begin{Vmatrix} \lambda & 0 \\ 0 & -1 \end{Vmatrix} \begin{Vmatrix} 1 & \alpha \\ 0 & 1 \end{Vmatrix} \begin{Vmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{Vmatrix} = \begin{Vmatrix} 1 & \lambda^2\alpha \\ 0 & 1 \end{Vmatrix}$$

y, en consecuencia, el normalizador $N(P)$ contiene el subgrupo

$$H = \left\{ \begin{Vmatrix} \lambda & \alpha \\ 0 & \lambda^{-1} \end{Vmatrix} \,\middle|\, \alpha, \lambda \in Z_p \ \ \lambda \neq 0 \right\}$$

de orden $p(p-1)$, entonces, queda la única posibilidad

$$N(P) = H, \quad N_p = 1 + p.$$

Entre el grupo

$$SL(2, Z_2) = \left\{ \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \begin{Vmatrix} 1 & 1 \\ 1 & 0 \end{Vmatrix}, \begin{Vmatrix} 0 & 1 \\ 1 & 1 \end{Vmatrix}, \right.$$

$$\left. \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}, \begin{Vmatrix} 1 & 0 \\ 1 & 1 \end{Vmatrix}, \begin{Vmatrix} 1 & 1 \\ 1 & 0 \end{Vmatrix} \right\}$$

y el grupo simétrico S_3, inmediatamente se establece el isomorfismo

$$(1\ 2\ 3) \mapsto \begin{Vmatrix} 1 & 1 \\ 1 & 0 \end{Vmatrix}, \quad (1\ 2) \to \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}$$

(ambos grupos tienen la misma tarea con generadores y relaciones). Para $p > 2$, el grupo $G = SL(2, Z_p)$, tiene centro $Z(G) = \{\pm E\}$ de orden 2. El grupo cociente $PSL(2, Z_p) = G/Z(G)$, al que es natural denominarlo grupo especial proyectivo (él es grupo de transformaciones de la recta proyectiva $Z_pP^1 = P^1(\ ) = \{0, 1, \ldots, p-1\} \cup \{\infty\}$), desempeña un papel importante en el álgebra desde los tiempos de Galois. La cuestión es, que cuando $p > 3$, el grupo $PSL(2, Z_p)$ es simple y, junto con A_n, es uno de los primeros ejemplos de grupos simples finitos.

Recurramos de nuevo al caso general y obtengamos una especificación útil de los teoremas de Sílov.

TEOREMA 1. *Son justas las afirmaciones sigientes:*

(i) *el p-subgrupo de Sílov P del grupo G es normal en G si, y sólo si,* $N_p = 1$;

(ii) *para que el grupo finito G de orden* $|G| = p_1^{n_1} \ldots p_k^{n_k}$ *resulte un producto directo de sus* p_i*-subgrupos de Sílov* $P_1, \ldots, P_k$, *es necesario y suficiente, que todos estos subgrupos sean normales en G.*

DEMOSTRACION. (i) Todos los subgrupos de Sílov, que responden a un divisor primo p dado de orden $|G|$, según el segundo teorema, son conjugados y, si P es uno de estos subgrupos, entonces, $N_p = 1 \Leftrightarrow xPx^{-1} = P,\ \forall x \in G \Leftrightarrow P \lhd G$.

(ii) Si $G = P_1 \times \ldots \times P_k$ es producto directo de sus subgrupos de Sílov, entonces, $P_i \lhd G$ es como cualquier multiplicador directo. Por lo tanto, la condición de normalidad es necesaria.

Sea ahora $P_i \lhd G$, $1 \leqslant i \leqslant k$, o sea, $N_{p_i} = 1$. Observemos, primero, que

$$x \in P_i \cap P_j, \quad i \neq j \Rightarrow x^{p_i^s} = e, \quad x^{p_j^t} = e \Rightarrow x = e.$$

Por lo tanto, $P_i \cap P_j = e$, de donde, para cualquier $x_i \in P_i$, $x_j \in P_j$, tenemos

$$[x_i, x_j] = \begin{cases} (x_i x_j x_i^{-1}) x_j^{-1} = x_j' x_j^{-1} \in P_j \\ x_i (x_j x_i^{-1} x_j^{-1}) = x_i x_i' \in P_i \end{cases} \Rightarrow [x_i, x_j] = e,$$

o sea, los elementos x_i y x_j son permutables.

Supongamos por un minuto, que el elemento unidad $e \in G$ está escrito en la forma $e = y_1 y_2 \ldots y_k$, donde $y_i \in P_i$, es un elemento de orden $a_i = p_i^{b_i}$. Haciendo $a = \prod_{i \neq j} a_i$ y aprovechando la permutabilidad de $y_1, \ldots, y_k$ obtenemos

$$e = (y_1 y_2 \ldots y_k)^a = y_1^a y_2^a \ldots y_k^a = y_j^a.$$

Pero, como a y a_j son primos entre sí, entonces, $y_j^{a_j} = y_j^a = e \Rightarrow y_j =$

$= e$. Esto es cierto para cualquier j, y, por lo tanto, la igualdad $e = y_1 y_2 \ldots y_k$ sólo es posible cuando $y_1 = y_2 = \ldots = y_k = e$.

Por otra parte, cada elemento $x \in G$ de orden $r = r_1 r_2 \ldots r_k$, $r_i = p_i^{s_i}$, se escribe en la forma

$$x = x_1 x_2 \ldots x_k, \quad |\langle x_i \rangle| = r_i, \quad 1 \leqslant i \leqslant k. \tag{7}$$

Es suficiente hacer $x_i = x^{t_i r_i'}$, donde los exponentes se definen mediante las condiciones

$$r_i' = r/r_i, \quad 1 = \sum_{i=1}^{k} t_i r_i'.$$

Si ahora $x = x_1' x_2' \ldots x_k'$ es otra escritura de x en forma de producto de p_i-elementos, entonces, en virtud de la permutabilidad de x_i, x_i' con diversos índices inferiores, tendremos

$$e = (x_1' x_2' \ldots x_k')(x_1 x_2 \ldots x_k)^{-1} = x_1' x_1^{-1} \cdot x_2' x_2^{-1} \ldots x_k' x_k^{-1},$$

que, como se indicó más arriba, conlleva a la igualdad $x_1' x_1^{-1} = x_2' x_k^{-1} = \ldots = x_k' x_k^{-1} = e$, o sea, $x_1' = x_1'$, $x_2' = x_2, \ldots, x_k' = x_k$.

Y bien, cada elemento del grupo G se expresa, sea dicho, de un modo único, en la forma (7), o sea (véase el § 3), $G = P_1 \times \ldots \times P_k$. ■

Observación. El p-subgrupo de Sílov normal P del grupo G, *es característico* en G, o sea, invariante para la operación de cualquier automorfismo $\varphi \in \mathrm{Aut}(G)$. Efectivamente, $|\varphi(P)| = |P|$, por eso, $\varphi(P)$ es un p-subgrupo de Sílov y, por lo tanto, $\varphi(P) = P$, si $N_p = 1$. Es también digno de mención, que los análogos de los subgrupos de Sílov se observan en estructuras algebraicas, lejanas a los grupos finitos.

EJERCICIOS

1. Hallar el número de los 5-subgrupos de Sílov en A_5.

2. Comprobar que el conjunto P de las matrices

$$\pm\begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \quad \pm\begin{Vmatrix} -1 & -1 \\ -1 & -1 \end{Vmatrix}, \quad \pm\begin{Vmatrix} -1 & -1 \\ -1 & 1 \end{Vmatrix}, \quad \pm\begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}$$

sobre Z_3 forma un grupo isomorfo al grupo de cuaterniones Q_8 y que es 2-subgrupo de Sílov en $SL(2, Z_3)$. Mostrar que $P \lhd SL(2, Z_3)$.

3. Mostrar que los grupos S_4 y $SL(2, Z_3)$ no son isomorfos. ¿Serán o no isomorfos los grupos $PSL(2, Z_3)$ y A_4?

4. Demostrar, que todo grupo G de orden pq ($p < q$, son números primos) es, bien cíclico, bien no abeliano con q-subgrupos de Sílov normal, además, esto último es posible si, y sólo si, $q - 1$ se divide por p. En particular, todos los grupos de orden 15 es cíclico.

5. Obtener nuevamente (véase el § 3, cap. 6) la congruencia $(p-1)! + 1 \equiv 0 \pmod{p}$ para el primo p, por medio del cálculo directo del número N_p de los p-subgrupos de Sílov en el grupo simétrico S_p.

§ 5. GRUPOS ABELIANOS FINITOS

En el grupo abeliano, todos los subgrupos son normales. De este hecho evidente y del teorema 4 del § 4, se deduce inmediatamente, que cualquier grupo abeliano A, de orden $|A| = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$, permite la descomposición

$$A = A(p_1) \times A(p_2) \times \ldots \times A(p_k) \qquad (1)$$

en el producto directo de sus subgrupos de Sílov $A(p_i)$. Los factores directos $A(p_1), \ldots, A(p_k)$ frecuentemente se llaman *componentes primarios* de grupo abeliano. La descomposición (1) está definida unívocamente: *cada componente $A(p_i)$ es sencillamente un conjunto de todos los p_i-elementos* (elementos en A, cuyos órdenes, sirven de potencia del número primo p_i).

Nuestra finalidad consiste en presentar el grupo abeliano A en forma de un producto directo de grupos elementales, como lo son los cíclicos. Si no se impone ninguna limitación a los órdenes de los grupos cíclicos, entonces, la condición de univocidad de esta descomposición es imposible de cumplir, como lo muestra el sencillo ejemplo:

$$A = \langle a \mid a^6 = e \rangle = \langle a^3 \rangle \times \langle a^2 \rangle.$$

Sin embargo, la posibilidad de arbitrariedades en la descomposición es bastante limitada, de modo que el resultado final (teorema 3) parece totalmente satisfactorio.

1. Grupos abelianos primarios. En adelante tendremos en cuenta, que si el grupo abeliano A es engendrado por sus subgrupos B, C, entonces, en realidad, $A = BC$; además, $A = B \times C$ si, y sólo si, $B \cap C = e$ (véase p. 4, § 3).

A diferencia del caso general, el grupo cíclico C_p^n de orden p^n es indescomponible, o sea, no se puede representar en forma de producto directo de grupos cíclicos de menor orden. En efecto, si $C_{p^n} = \langle a \rangle$ y $C_{p^i} = \langle a^{p^{n-i}} \rangle$, entonces, en la cadena

$$C_{p^n} \supset C_{p^{n-1}} \supset \ldots \supset C_p \supset e$$

se ecuentran todos los subgrupos del grupo C_{p^n}. Cualesquiera dos de ellos $X \neq e$, $Y \neq e$ poseen una intersección no trivial $X \cap Y \supset \supset C_p$ y, por eso, no pueden servir de componentes de una descomposición directa.

TEOREMA 1 *Cada p-grupo abeliano finito es producto directo de grupos cíclicos.*

DEMOSTRACIÓN Razonando por inducción y suponiendo demostrado el teorema para todos los p-grupos abelianos de orden $<p^n$, elegimos en nuestro grupo A, $|A| = p^n$, el elemento $a \neq e$ de máximo orden p^m y pasamos al grupo cociente $\overline{A} = A/\langle a \rangle$. Como

$|\bar{A}| = p^{n-m} < p^n$, entonces, por presupuesto de la inducción

$$\bar{A} = \bar{A}_1 \times \ldots \times \bar{A}_r. \qquad (2)$$

donde $\bar{A}_i = \langle \bar{b}_i \rangle - \langle b_i \langle a \rangle \rangle = \{\langle a \rangle, \ b_i \langle a \rangle, \ \ldots, \ b_i^{p^{m_i}} \langle a \rangle\}$ es un grupo cíclico de orden p^m, $1 \leqslant i \leqslant r$, $m_1 + \ldots + m_r = n - m$. Por definición

y, aunque cada elemento $x \in A$ tiene la forma

$$\bar{b}_i^{p^{m_i}} = \bar{e} = \langle a \rangle, \quad \text{o sea,} \quad b_i^{p^{m_i}} = a^{s_i} \in \langle a \rangle, \qquad (3)$$

$$x = b_1^{k_1} \ldots b_r^{k_r} \cdot a^k,$$

esta escritura, hablando en general, no es única. Debemos «corregir» los elementos $b_i \in A$ de modo tal, que los exponentes s_i en (3) sean iguales a cero. No es difícil hacer esto. Recordando que $m_i \leqslant m$ y elevando ambos miembros de la relación (3) a la potencia p^{m-m_i}, obtendremos

$$e = a^{s_i p^{m-m_i}},$$

de donde, $s_i = t_i p^{m_i}$ (teorema 3, § 2, cap. 4). Si ahora se hace $a_i = b_i a^{-t_i}$, entonces, (3) se convierte en la relación

$$a_i^{p^{m_i}} = e, \quad 1 \leqslant i \leqslant r \ (\Longleftrightarrow \langle a_i \rangle \cap \langle a \rangle = e), \qquad (3')$$

además, $a_i = a_i \langle a \rangle = b_i \langle a \rangle = \bar{b}_i$, y, en consecuencia, $\langle \bar{a}_i \rangle = \bar{A}_i$. Nuevamente

$$x = a_1^{k_1} \ldots a_r^{k_r} a^k$$

para cualquier $x \in A$, y esta expresión es ahora única. En caso contrario se obtiene la relación

$$a_1^{\nu_1} \ldots a_r^{\nu_r} a^{\nu} = e, \quad 0 \leqslant \nu_i < p^{m_i}, \quad 0 \leqslant \nu < p^m,$$

(no todos los ν_i, ν son nulos), a la que, para el epimorfismo $A \to \bar{A}$, corresponde la relación $\bar{a}_1^{\nu_1} \ldots \bar{a}_r^{\nu_r} = \bar{e}$. En condiciones de la descomposición directa (2), ella es equivalente al sistema $\bar{a}_i^{\nu_i} = \bar{e}$, $1 \leqslant i \leqslant r$, o, lo que es igual, $a_i^{\nu_i} \in \langle a \rangle$. Pero, de acuerdo con (3′), esto sólo es posible cuando $\nu_i = 0$, pero, entonces también $\nu = 0$. La contradicción obtenida muestra que

$$A = \langle a_1 \rangle \times \ldots \times \langle a_r \rangle \times \langle a \rangle. \quad \blacksquare$$

Observación. La demostración del teorema 1 expuesta, se asemeja a la demostración geométrica del teorema sobre la forma normal de Jordan de la matriz del operador lineal nilpotente (véase el complemento).

De complemento importante al teorema 1, sirve el

TEOREMA 2. *Si el p-grupo abeliano finito A se descompone de dos modos en producto directo de subgrupos cíclicos:*

$$A = A_1 \times \ldots \times A_r = B_1 \times \ldots \times B_s,$$

entonces, $r = s$ y los órdenes de $|A_i|$ coinciden con los de $|B_j|$, con cierto ordenamiento de los últimos.

DEMOSTRACIÓN. Cuando $|A| = p$ el teorema, evidentemente, es cierto. Utilicemos la inducción sobre $|A|$. Es cómodo ordenar desde un principio los componentes A_i y B_j de tal modo, que sus órdenes no sean crecientes:

$$A_i = \langle a_i \rangle \mid \langle a_i \rangle \mid = p^{m_i},$$
$$m_1 \geqslant m_2 \geqslant \ldots \geqslant m_q > m_{q+1} = \ldots = m_r = 1; \qquad (4)$$
$$B_j = \langle b_j \rangle, \quad |\langle b_j \rangle| = p^{n_j},$$
$$n_1 \geqslant n_2 \geqslant \ldots \geqslant n_t > n_{t+1} = \ldots = n_s. \qquad (5)$$

De las relaciones

$$(xy^p) = x^p y^p, \quad (x^p)^{-1} = (x^{-1})^p,$$

legítimas en cualquier grupo abeliano (véase (3), § 1, cap. 4), se deduce que el conjunto

$$A^p = \{x^p \mid x \in A\}$$

de los $p-x$ grados de todos los elementos de A, forma un subgrupo en A, independiente de cualquier descomposición de A en producto directo. Por otro lado, si

$$a_1^{i_1} \ldots a_q^{i_q} \ldots a_r^{i_r} = x - b_1^{j_1} \ldots b_t^{j_t} \ldots b_s^{j_s},$$

entonces, teniendo en cuenta (4) y (5), tenemos

$$(a_1^p)^{i_1} \ldots (a_q^p)^{i_q} = x^p = (b_1^p)^{j_1} \ldots (b_t^p)^{j_t}.$$

Por lo tanto,

$$\langle \tilde{a}_1 \rangle \times \ldots \times \langle \tilde{a}_q \rangle = A^p = \langle \tilde{b}_1 \rangle \times \ldots \times \langle \tilde{b}_t \rangle,$$

donde $\tilde{a}_i = a_i^p$, $\tilde{b}_j = b_j^p$, son elementos de órdenes p^{m_i-1} y n^{n_j-1} respectivamente. Como $|A^p| < |A|$, entonces, por presupuesto de la inducción, $q = t$ y $m_1 - 1 = n_1 - 1, \ldots, m_q - 1 = n_q - 1$, de donde $m_1 = n_1, \ldots, m_q = n_q$. Observando también, que

$$|A_{q+1} \times \ldots \times A_r| = p^{r-q}, \quad |B_{t+1} \times \ldots \times B_s| = p^{s-t}, \quad q = t,$$

obtenemos

$$p^{m_1+\cdots+m_q} p^{r-q} = |A| = p^{m_1+\cdots+m_q} p^{s-q}.$$

Por consiguiente, $s = r$, y todas las afirmaciones del teorema han sido demostradas.

Los órdenes $p^{m_1}, \ldots, p^{m_r}$ de los multiplicadores directos cíclicos se llaman *invariantes* (o *divisores elementales*) del p-grupo abeliano finito A. Si dos grupos abelianos A, B, tienen los mismos invariantes, entonces,

$$A = A_1 \times \ldots \times A_r, \quad B = B_1 \times \ldots \times B_r, \quad A_i \cong C_{p^{m_i}} \cong B_i,$$

y el sistema de aplicaciones isomorfas φ_i: $A_i \to B_i$, induce el isomorfismo φ: $\varphi((a_1, \ldots, a_r)) = (\varphi_1(a_1), \ldots, \varphi_r(a_r))$ entre los grupos A y B. Por lo tanto, el teorema 2 dice que el *grupo A se determina con exactitud hasta el isomorfismo por medio de sus invariantes.* En particular, cabe el

COROLARIO. *El número de grupos abelianos no isomorfos de orden p^n, es igual al número $p(n)$ de particiones*

$$n = n_1 + n_2 + \ldots + n_r, \quad n_1 \geqslant n_2 \geqslant \ldots \geqslant n_r \geqslant 1,$$
$$1 \geqslant r \geqslant n. \blacksquare$$

La función de números enteros $p(n)$ fue tratada por nosotros durante la descripción de las clases de elementos conjugados en el grupo simétrico S_n (véase el ejercicio 4 del § 2). El grupo abeliano de orden p^r con invariantes $p, \ldots, p$, habitualmente se llama *grupo abeliano elemental*. Este grupo A se caracteriza por la condición $A^p = e$. Dando preferencia a la escritura aditiva, observamos que el grupo abeliano A, con $pA = 0$ (p es un número primo), es un espacio vectorial sobre el campo finito $\mathbb{F}_p$ de p elementos. En efecto, si los elementos de $\mathbb{F}_p$ se identifican con las clases de restos $\bar{k}$ respecto al módulo p ($\mathbb{F}_p = Z_p$) y se hace $\bar{k}a = ka$, $a \in A$, entonces, llegaremos a provocar la operación $\mathbb{F}_p$ sobre A, que transforma a A en un espacio vectorial sobre $\mathbb{F}_p$. Esta operación está definida correctamente, porque de $\bar{k} = \bar{k}'$ sigue $(k - k')a = l(pa) = 0$. La descomposición de A en una suma directa de subespacios cíclicos corresponde a la descomposición del espacio vectorial en una suma directa de subespacios unidimensionales (teorema sobre la base). Así,

$$A \cong Z_p^r = Z_p \oplus \ldots \oplus Z_p.$$

Cuan grande es la arbitrariedad en la elección de los espacios básicos unidimensionales, incluso cuando $r = 2$, se aprecia del ejemplo en el § 4: Z_p^2 permite $p(p+1)$ descomposiciones distintas.

2. **Teorema fundamental sobre grupos abelianos finitos.** Haciendo hincapié en la descomposición (1) y en su unicidad, así como en los teoremas 1 y 2, llegamos inmediatamente a la afirmación fundamental sobre los grupos abelianos siguiente.

TEOREMA 3 *Todo grupo abeliano finito A es producto directo de subgrupos cíclicos primarios. Cualesquiera dos descomposiciones de este tipo tienen cada una el mismo número de multiplicadores de cada orden.*

Adoptando la terminología de la teoría de espacios vectoriales, diremos que los elementos $a_1, \ldots, a_r$, de órdenes $d_1, \ldots, d_r$, componen la *base* del grupo abeliano A, si cada elemento $x \in A$ se escribe de un modo único en la forma

$$x = a_1^{i_1} a_2^{i_2} \ldots a_r^{i_r}, \quad 0 \leqslant i_k \leqslant d_k, \quad k = 1, \ldots, r.$$

Por supuesto, en tal caso

$$A = \langle a_1 \rangle \times \ldots \times \langle a_r \rangle, \quad |A| = d_1 d_2 \ldots d_r, \tag{6}$$

y el teorema 3 es equivalente a la afirmación sobre la existencia, en todo grupo abeliano finito A, de una base con elementos primarios (o sea, los órdenes d_i de los mismos, son potencias de los primos p, divisores de $|A|$) además, el sistema $\{d_1, d_2, \ldots, d_r\}$ no depende de la elección de la base. Por esta razón, como en el caso de los grupos primarios, los números $d_1, \ldots, d_r$ se llaman *invariantes* o *divisores elementales* del grupo A. A veces también se dice que $\{d_1, \ldots, d_r\}$ son el *tipo* del grupo abeliano finito A.

Indiquemos todos los invariantes, colocándolos en filas que responden a diferentes divisores primos de orden $|A|$:

$$\begin{array}{llll} p_1^{n_{11}}, & p_1^{n_{12}}, & p_1^{n_{13}}, \ldots; & n_{11} \geqslant n_{12} \geqslant n_{13} \geqslant \ldots; \\ p_2^{n_{21}}, & p_2^{n_{22}}, & p_2^{n_{23}}, \ldots; & n_{21} \geqslant n_{22} \geqslant n_{23} \geqslant \ldots; \\ \ldots & \ldots & \ldots & \ldots \\ p_k^{n_{k1}}, & p_k^{n_{k2}}, & p_k^{n_{k3}}, \ldots; & n_{k1} \geqslant n_{k2} \geqslant n_{k3} \geqslant \ldots \end{array}$$

Puede considerarse que todas las filas tienen la misma longitud l, si se completan algunas de éstas con unidades.

Los números enteros

$$m_j = p_1^{n_{1j}} p_2^{n_{2j}} \ldots p_k^{n_{kj}}, \quad j = 1, 2, \ldots, l,$$

se llaman *factores* (o *multiplicadores*) *invariantes* del grupo abeliano A. Por construcción

$$|A| = m_1 m_2 \ldots m_l, \quad m_{j+1} \mid m_j, \quad j = 1, 2, \ldots, l-1. \tag{7}$$

De la descomposición (6), reescrita en la forma

$$A = (\langle a_{11} \rangle \times \ldots \times \langle a_{k1} \rangle) \times \ldots \times (\langle a_{1l} \rangle \times \ldots \times \langle a_{kl} \rangle),$$

pasamos ahora a la descomposición

$$A = \langle u_1 \rangle \times \langle u_2 \rangle \times \ldots \times \langle u_l \rangle \tag{8}$$

con multiplicadores cíclicos directos de órdenes $m_1, m_2, \ldots, m_l$. Para eso, es suficiente hacer

$$u_j = a_{1j} a_{2j} \ldots a_{kj}, \quad 1 \leqslant j \leqslant l,$$

y alegar la proposición del final del p. 3, § 2, cap. 4.

Para el grupo primario A, las descomposiciones directas (6) y (8), evidentemente, coinciden, pero, en el caso general, la (8) es más breve que la (6) ($l \leqslant r \leqslant kl$), además, en (8) se separa de inmediato el elemento u_1 de mayor orden m_1; los órdenes de los demás elementos del grupo A dividen el primer factor invariante m_1. El número entero m_1 se denomina también *índice* (o *exponente*) del

grupo A. *El grupo abeliano A es cíclico si, y sólo si, su índice coincide con el orden de $|A|$.*

Queda por agregar, que la cuestión sobre la existencia del grupo abeliano A con los factores invariantes dados $m_1, m_2, \ldots, m_t$, no surge: es suficiente examinar (en escritura aditiva) la suma directa de los grupos cíclicos $Z_{m_1}, \ldots, Z_{m_t}$.

En calidad de ejemplo, enumeremos todos los grupos abelianos de órdenes 16 y 36.

$$|A| = 16 = 2^4, \quad p(4) = 5: \; Z_{16}, \quad Z_8 \oplus Z_2,$$
$$Z_4 \oplus Z_4, \quad Z_4 \oplus Z_2 \oplus Z_2, \quad Z_2^4 = Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2$$

$\lvert A \rvert = 36 = 2^2 \cdot 3^2$	Divisores elementales	Factores invariantes
$Z_4 \oplus Z_9 \cong Z_{36}$	4, 9	36
$Z_2 \oplus Z_2 \oplus Z_9 \cong Z_{18} \oplus Z_2$	2, 2, 9,	18,2
$Z_4 \oplus Z_3 \oplus Z_3 \cong Z_{12} \oplus Z_3$	4, 3, 3,	12,3
$Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_3 \cong Z_6 \oplus Z_6$	2, 2, 3, 3	6,6

Consideremos otro ejemplo más. Indiquemos el grupo $Z_{72} \oplus Z_{84}$ en términos de factores invariantes. Al principio, cada uno de los sumandos cíclicos los expresaremos por medio de los componentes primarios cíclicos:

$$Z_{72} = Z_8 \oplus Z_9, \quad Z_{84} = Z_4 \oplus Z_3 \oplus Z_7$$

Luego, unamos todos los componentes primarios

$$Z_{72} \oplus Z_{84} = (Z_8 \oplus Z_4) \oplus (Z_9 \oplus Z_3) \oplus Z_7$$

(suma directa de p-subgrupos de Sílov). Ahora queda separar un sumando cíclico de orden máximo en cada componente primario, y repetir este proceso con los sumandos restantes:

$$Z_{72} \oplus Z_{84} = (Z_8 \oplus Z_9 \oplus Z_7) \oplus (Z_4 \oplus Z_3) = Z_{504} \oplus Z_{12}.$$

Si se hace lo mismo con el grupo $Z_{36} \oplus Z_{168}$, entonces, se obtendrá un resultado análogo.

En consecuencia,

$$Z_{72} \oplus Z_{84} = Z_{36} \oplus Z_{168}$$

(hablando en rigor en todos lados hubiese correspondido poner el signo $\cong$ en lugar del de igualdad). En particular, señalemos, que los índices de ambos grupos son iguales a 504.

EJERCICIOS

1. Demostrar el teorema 1 o incluso la primera parte del teorema 3, sin pasar a los factores cocientes. (*Indicación.* Se inicia del mismo modo. Luego, al grupo cíclico $\langle a \rangle$ de orden máximo m en A se le debe agregar el sumando directo máximo B. Si $\langle a \rangle \times B = A$, entonces, todo está demostrado. En caso contrario, examinar el elemento $c \in A$, no contenido en $\langle a \rangle \times B$, pero tal, que $c^p \in \langle a \rangle \times B$ para el exponente primo p. Los razonamientos ulteriores se efectúan en el grupo $\langle c, \langle a \rangle \times B \rangle$, procurando obtener para el mismo la descomposición $\langle a \rangle \times B'$, $B' \supset B$).

2. Obtener la descomposición del grupo abeliano finito A en componentes primarios, sin recurrir a los teoremas de Sílov y, por supuesto, no utilizando el teorema 3. En particular, para que siendo $n = d_1 d_2 \ldots d_k$, $d_i = p_i^{e_i}$ (p_i son diversos divisores primos), obtener la descomposición

$$Z_n \cong Z_{d_1} \oplus Z_{d_2} \oplus \ldots \oplus Z_{d_k}$$

del grupo cíclico $(Z_n, +)$, se puede utilizar el ejemplo 1 del p. 1, § 3, o la proposición del p. 3, § 2, cap. 4.

3. Mostrar, que en el grupo abeliano finito A, para cualquier $d \mid |A|$ existe por lo menos un subgrupo de orden d (giro del teorema de Lagrange).

4. Mostrar, que con un ordenamiento correspondiente los invariantes de cualquier subgrupo son divisores de los invariantes de un grupo abeliano.

5. Si $A \oplus A \cong B \oplus B$, donde A y B son grupos abelianos finitos, entonces, $A \cong B$.

6. Si A, B, C, son grupos abelianos finitos, y $A \oplus C \cong B \oplus C$, entonces, $A = B$.

7. Mostrar, que el grupo abeliano con factores invariantes $m_1, \ldots, m_l$, no puede ser engendrado por menos de l elementos.

8. El grupo abeliano finito de orden n, no divisible por el cuadrado de ningún número entero >1, es cíclico.

9. Hacer recuento de todos los grupos abelianos no isomorfos de orden 72

10. ¿Son isomorfos los grupos $Z_{12} \oplus Z_{72}$ y $Z_{18} \oplus Z_{48}$?

Capítulo 8

ELEMENTOS DE LA TEORÍA DE REPRESENTACIONES

A la definición exacta de la teoría de representaciones lineales de grupos, le anteponemos dos problemas cercanos por su espíritu.

PROBLEMA 1. En el espacio $(m+1)$-dimensional V_m de los polinomios reales homogéneos

$$f(x, y) = a_0x^m + a_1x^{m-1}y + \ldots + a_{m-1}y^{m-1}x + a_my^m$$

(o, más bien, de las funciones polinómicas $(x, y) \to f(x, y)$) de grado m, se separa el conjunto de soluciones de la *ecuación* bidimensional *de Laplace*
en derivadas parciales (véase el ejercicio 9, § 1, cap. 6). El operador

$$\frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} = 0 \qquad (*)$$

Por eso las soluciones de la ecuación $(*)$ forman cierto subespacio de Laplace $\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$ es lineal:

$$\Delta(\alpha f + \beta g) = \alpha\,\Delta f + \beta\,\Delta g, \qquad \alpha, \quad \beta \in \mathbb{R}.$$

Por eso, las soluciones de la ecuación $(*)$ forman cierto subespacio H_m del espacio V_m. Se comprueba inmediatamente, que

$$\Delta f = \sum_{k=0}^{m-2} [(m-k)(m-k-1)a_k + (k+2)(k+1)a_{k+2}]\,x^ky^{m-2-k}.$$

En consecuencia

$$\Delta f = 0 \Leftrightarrow (m-k)(m-k-1)a_k + (k+2)(k+1)a_{k+2} = 0, \quad 0 \leqslant k \leqslant m-2,$$

y todos los coeficientes a_k se expresan mediante dos de ellos, digamos, a_0 y a_1. De este modo, $\dim H_m \leqslant 2$.

Pero dos soluciones linealmente independientes se pueden indicar enseguida. Efectivamente, extendiendo respecto a la linealidad la acción del operador Δ a los polinomios con coeficientes complejos, tendremos

$$\Delta(x+iy)^m = m(m-1)(x+iy)^{m-2} + imi(m-1)(x+iy)^{m-2} = 0, \quad i^2 = -1.$$

Separando las partes entera e imaginaria, obtenemos

$$z_m(x, y) \equiv (x+iy)^m = u_m(x, y) + iv_m(x, y),$$

de donde

$$\Delta u_m + i\,\Delta v_m = \Delta z_m = 0 \Rightarrow \Delta u_m = 0, \quad \Delta v_m = 0.$$

Así,

$$H_m = \langle u_m(x, y), v_m(x, y)\rangle_{\mathbb{R}}.$$

Interpretando ahora x, y como coordenadas de un vector en el plano euclídeo $\mathbb{R}^2$ con un sistema de coordenadas cartesianas dado, veamos qué pasará con un cambio ortogonal de coordenadas, cuando se hace girar el plano $\mathbb{R}^2$ alrededor del punto de origen a un ángulo cualquiera θ:

$$x' = \Phi_0(x) = x\cos\theta - y\,\mathrm{sen}\,\theta,$$
$$y' = \Phi_\theta(y) = x\,\mathrm{sen}\,\nu + y\cos\theta.$$

La regla de diferenciación de funciones complejas, conocida del análisis (y fácil de comprobar para los polinomios), da

$$\frac{\partial^2 f}{\partial x'^2} = \frac{\partial^2 f}{\partial x^2}\cos^2\theta - 2\frac{\partial^2 f}{\partial x\,\partial y}\cos\theta\cdot\mathrm{sen}\,\theta + \frac{\partial^2 f}{\partial y^2}\mathrm{sen}^2\,\theta,$$
$$\frac{\partial^2 f}{\partial y'^2} = \frac{\partial^2 f}{\partial x^2}\cos^2\theta + 2\frac{\partial^2 f}{\partial x\,\partial y}\cos\theta\cdot\mathrm{sen}\,\theta + \frac{\partial^2 f}{\partial y^2}\mathrm{sen}^2\,\theta,$$

de donde

$$\frac{\partial^2 f}{\partial x'^2} + \frac{\partial^2 f}{\partial y'^2} = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2}.$$

Esto significa, que la ecuación (*) que da invariante frente a un cambio ortogonal de variables o, como también podríamos decir, con la operación del grupo SO (2) = Φ_θ. En particular, los polinomios $u_m(x', y')$, $v_m(x', y')$ serán soluciones de la ecuación (*) y como tales se expresarán linealmente mediante $u_m(x, y)$, $v_m(x, y)$. De esto modo, el grupo SO (2) opera en el espacio de soluciones de la ecuación de Laplace. En este caso se habla sobre la representación real lineal bidimensional

$$\Phi^{(m)}\colon \Phi_0 \to \Phi^{(m)}(\theta)$$

del grupo SO (2).

Volviendo de nuevo a los polinomios complejos, observamos que

$$x' + iy' = xe^{i\theta} + iye^{i\theta} = e^{i\theta}(x + iy),$$
$$(x' + iy')^m = e^{im\theta}(x + iy)^m.$$

Conservando para el operador lineal complejo $\Phi^{(m)}(\theta)$ su denotación anterior, tendremos

$$\Phi^{(m)}(\theta)\colon z_m \mapsto z'_m = e^{im\theta} z_m.$$

Las llamadas representaciones unitarias lineales $\Phi^{(m)}\colon \Phi_\theta \mapsto e^{im\theta}$, $m \in \mathbb{Z}$, del grupo SO (2) desempeñan un papel importante en el análisis.

Observemos, que la operación Φ induce la operación del grupo SO (2) en todo el espacio V_m y, desde este punto de vista H_m es un espacio invariante en V_m.

PROBLEMA 2. La evaluación del número de los posibles compuestos orgánicos, por ejemplo, en la química de hidrocarburos cíclicos, se reduce al problema vital-abstracto siguiente. ¿Cuántos collares

distintos de longitud n se puede formar, a partir de una reserva ilimitada de perlas q, de diferentes colores?

Tratemos de responder a esta pregunta (siguiendo a G. Poliá) considerando, que los collares están orientados, o sea, un collar dado vuelta, hablando en general, no se identifica con el original. Observemos, que el número total de segmentos de hilo con n perlas enhebradas que se tiene es q^n (número de palabras de longitud n en un subgrupo libre con q generadores). En el conjunto Ω_n de estos segmentos opera el grupo cíclico $\langle\sigma\rangle$ de orden n con el generador $\sigma = (12 \ldots n) \in S_n$, que permuta cíclicamente las perlas en cada segmento. Es natural considerar el collar como $\langle\sigma\rangle$-órbita del segmento o, si se desea, cierto conjunto de círculos concéntricos (fig. 21). La segunda interpretación es más evidente. Ella está vinculada con el isomorfismo

$$\Phi : \sigma \mapsto \Phi(\sigma) = \left\| \begin{matrix} \cos \frac{2\pi}{n} & -\operatorname{sen} \frac{2\pi}{n} \\ \operatorname{sen} \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{matrix} \right\|,$$

con el que antes ya hemos encontrado, y que más tarde llamaremos representación real lineal bidimensional del grupo $\langle\sigma\rangle$. El número buscado de r collares se expresa mediante la fórmula del ejercicio 5, § 2, cap. 4

$$r = \frac{1}{n} \sum_{k=0}^{n-1} N(\sigma^k).$$

Si $d \mid n$, entonces, el elemento σ^d de orden n/d deja en sus lugares aquellos segmentos (y collares) que se disponen en d períodos de longitud n/d (en relación con esto, véase el ejercicio 13, § 2, del cap. 4). Por eso, $N(\sigma^d) = q^d$, y $N(\sigma^k) = q^{\text{m.c.d.}(n,k)}$. A la magnitud $N(\sigma\ )$ con m.c.d. $(n, k) = d$ en la suma $\sum N(\sigma^k)$ le corresponde exactamente $\varphi\left(\frac{n}{d}\right)$ sumandos (φ es la función de Euler). Esto significa, que

$$r = \frac{1}{n} \sum_{d \mid n} \varphi\left(\frac{n}{d}\right) q^d.$$

El paso a collares físicamente distintos (no orientados) está ligado con identificaciones complementarias de los elementos en Ω_n, mediante una representación lineal bidimensional corriente del grupo diedral D_n. Procure hacer esto independientemente.

No sólo en los ejemplos examinados, sino que también en problemas físicos concretos las representaciones lineales de grupos, aparecen arbitrariamente, como reflejo de una u otra simetría. La idea y la lengua de la teoría de representaciones son, respectivamente, muy naturales. Así, los ejemplos expuestos en el § 1, se refieren a

problemas bien conocidos y al parecer no aportan nada nuevo. Sin embargo, el propio hecho de que se encuentren «bajo un mismo techo» debe conducir a reflexiones útiles.

La finalidad perseguida por la teoría de representaciones es doble: 1) puramente matemática, dictada en parte por el deseo de emplear un aparato complementario para la investigación de los

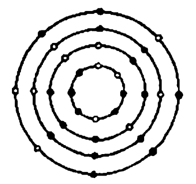


Fig. 21

propios grupos, 2) aplicada, ilustrada, digamos, por su gran contribución a la cristalografía y a la mecánica cuántica. Ninguno de estos aspectos en esencia, está reflejado en el presente capítulo, cuyo fin es más que modesto: decir algo interesante sobre la teoría de representaciones, basándonos exclusivamente en un material que nos es accesible, proveniente del álgebra lineal y de la teoría de los grupos.

§ 1. DEFINICIÓN Y EJEMPLOS DE REPRESENTACIONES LINEALES

1. Conceptos fundamentales. Hablando con propiedad, ya hemos estudiado la teoría de representaciones cuando consideramos (en el § 2, cap. 7) la operación de grupos en los conjuntos. Tomemos ahora en calidad de conjunto el espacio vectorial V de dimensión n sobre el campo K y separemos en el grupo $S(V)$, de todas las transformaciones biyectivas $V \rightarrow V$ del subgrupo $\mathrm{GL}(V)$, que es el grupo de los operadores lineales invertibles en V (o grupo de automorfismos del espacio V). Es claro, que para cualquier elección de la base $\{e_1, \ldots, e_n\}$ en V, el grupo $\mathrm{GL}(V)$ se vuelve un grupo matricial común $\mathrm{GL}(N, K)$, que puede considerarse grupo de automorfismos del espacio lineal aritmético K. Con esto, a cada operador lineal $\mathcal{A} \in \mathrm{GL}(V)$, le corresponde una matriz $A = (a_{ij})$ tal, que

$$\mathcal{A}e_j = \sum_{i=1}^{n} a_{ij}e_i; \quad a_{ij} \in K, \quad \det A \neq 0.$$

DEFINICIÓN 1. Sea G algún grupo. Todo homomorfismo $\Phi\colon G \rightarrow \mathrm{GL}(V)$ se llama *representación lineal* del grupo G en el espacio V. La representación se denomina *exacta*, si su *núcleo* $\mathrm{Ker}\,\Phi$ sólo está compuesto por el elemento unidad del grupo G, y *trivial* (o *unidad*)

si $\Phi(g) = \mathscr{E}$ es un operador unidad para todo elemento $g \in G$. La dimensión $\dim_K V$, también se denomina *grado de la representación*. Para $K = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, se habla, respectivamente, sobre una representación racional, real o compleja del grupo G.

De este modo, la representación lineal es un par (Φ, V), compuesto del *espacio de representación* V (o *G-espacio*) y del homomorfismo $\Phi: G \to \mathrm{GL}(V)$. Por definición

$$\Phi(e) = \mathscr{E} \text{ es un operador unidad;}$$

$$\Phi(gh) = \Phi(g)\,\Phi(h) \text{ para todo } g,\ h \in G.$$

Conviniendo en designar por $g * v$ la operación del operador lineal $\Phi(g)$ sobre el vector $v \in V$, llegamos a las relaciones

$$\begin{aligned} g * (u + v) &= g * u + g * v, \quad u, v \in V, \\ g * (\lambda v) &= \lambda (g * v), \quad \lambda \in K, \\ e * v &= v, \\ (gh) * v &= g * (h * v), \end{aligned} \tag{1}$$

que imitan las propiedades de los operadores lineales, además, las dos últimas relaciones sustituyen lo que antes se expresó con el signo Φ (comparar con (i), (ii) en el § 2 del cap. 7). Las relaciones (1) en la representación lineal (Φ, V) llevan a un primer lugar el G-espacio V, lo que a veces es cómodo hacer por unas u otras razones (por ejemplo, cuando V no es un espacio lineal abstracto, sino alguna realización concreta del mismo).

Por otra parte, el espacio V puede no mencionarse, si por representación lineal se comprende sencillamente el homomorfismo Φ del grupo G en el grupo matricial $\mathrm{GL}(n, K)$. Como antes, $\Phi_{gh} = \Phi_g \Phi_h$, pero aquí Φ_g es una matriz no degenerada, además, $\Phi_e = E$ es una matriz unidad. La interpretación matricial es preferible desde el punto de vista del cálculo, pero es menos invariante y carece de evidencia espacial. De hecho, es importante dominar el arte (simple) de pasar libremente de representaciones G-espaciales a matriciales y viceversa.

En relación a esto, recordemos el hecho, bien conocido del curso de álgebra lineal, que dos matrices A, B, que responden a un mismo operador lineal en distintas bases, son semejantes: $B = CAC^{-1}$ (C es la matriz de paso de una base a otra). En el caso de representaciones, cuando se habla sobre el grupo de operadores lineales, la dependencia de la elección de la base, se toma en cuenta del modo siguiente.

DEFINICIÓN 2. Dos representantes lineales (Φ, V), (Ψ, W) del grupo G se llaman *equivalentes* (*isomorfas* o *semejantes*), si existe un isomorfismo de los espacios vectoriales $\sigma: V \to W$, que vuelve al

diagrama

$$\begin{array}{ccc} V & \xrightarrow{\sigma} & W \\ {\scriptstyle \Phi(g)}\downarrow & & \downarrow{\scriptstyle \Psi(g)} \\ V & \xrightarrow{\sigma} & W \end{array}$$

conmutativo para todo $g \in G$, o sea,

$$\Psi(g)\,\sigma = \sigma\Phi(g), \quad g \in G,$$

o, lo que resulta equivalente,

$$\Psi(g) = \sigma\Phi(g)\,\sigma^{-1} \qquad (2)$$

(comparar con la definición de equivalencia de las operaciones de los grupos en los conjuntos, dada en el ejercicio 1, § 2, cap. 7). A veces, escribiremos $\Phi \approx \Psi$ para las representaciones equivalentes, y $\Phi \approx \Psi$ para las no equivalentes.

Enunciemos dos variantes más de la definición 2.

a) TERMINOLOGIA MATRICIAL. Sean G un grupo, y V: $(g, v) \mapsto q * v$, W: $(g, w) \mapsto g \square w$, dos G-espacios con operciones $*$, $\square$, que satisfacen la condición (1). El isomorfismo σ: $V \to W$ de los espacios vectoriales, es un *isomorfismo G-espacial*, si

$$g \square \sigma(v) = \sigma(g * v) \qquad (2')$$

para todo $g \in G$ y $v \in V$. También se dice, que la aplicación σ es permutable con la operación G.

b) TERMINOLOGIA G-ESPACIAL. Si $V = \langle v_1, \ldots, v_n \rangle$, $W = \langle w_1, \ldots w_n \rangle$ y Φ_g, Ψ_g son las matrices de los operadores lineales $\Phi(g)$, $\Psi(g)$ respecto a las bases elegidas, entonces, la condición de equivalencia (2) se expresa en la forma

$$\Psi_g = C\Phi_g C^{-1}, \qquad (2'')$$

donde C es cierta matriz no degenerada, la misma para todo $g \in G$. Los coeficientes de todas las matrices examinadas, pertenecen a un campo K.

La relación de semejanza de matrices, expresada por la condición (2″), es la relación de equivalencia que divide al conjunto $M_n(K)$ en clases disjuntas. En correspondencia, las representaciones del grupo G también se parten en clases de representaciones equivalentes. Más adelante quedará claro, que para la teoría de representaciones son interesantes y esenciales, precisamente las clases de representaciones equivalentes.

Recurriendo nuevamente al curso de álgebra lineal, intentemos darnos una idea más evidente de la operación del grupo $\Phi(G)$ en el espacio V. Con relación al operador lineal $\mathcal{A}$: $V \to V$ en V puede existir el subespacio invariante U: $u \in U \Rightarrow \mathcal{A}u \in U$. Completando la base arbitraria $\{e_1, \ldots, e_h\}$ en U, hasta la base de todo el espacio

$V = \langle e_1, \ldots, e_k, e_{k+1}, \ldots, e_n \rangle$, veremos, que la matriz del operador $\mathcal{A}$ en la base $\{e_1, \ldots, e_n\}$, tomará la forma triangular en bloques:

$$A = \begin{Vmatrix} A_1 & A_0 \\ 0 & A_2 \end{Vmatrix}.$$

El bloque A_1 corresponde al subespacio invariante U, y el bloque A_2 al espacio cociente V/U. Si A_0 es una matriz nula, entonces, $A = A_1 + A_2$ es la suma directa de los bloques, y $V = U \oplus W$ es la suma directa de los subespacios invariantes.

La existencia de un subespacio invariante propio respecto a $\mathcal{A}$ está siempre asegurada, ya que el campo básico K es algebraicamente cerrado (véase el § 3, cap. 6). Si, por ejemplo, $K = \mathbb{C}$ es un campo de números complejos, entonces, habrá un vector $v \in V$, $v \neq 0$, para el cual, $\mathcal{A}v = \lambda v$. Aquí λ es raíz del polinomio característico

$$f_{\mathcal{A}}(t) = | tE - A | = t^n - (\operatorname{tr} A)\, t^{n-1} + \ldots + (-1)^n \det A$$

(A es una matriz arbitraria del operador lineal $\mathcal{A}$). Este razonamiento permite elegir una base en V, respecto a la cual A toma la forma triangular

$$A = \begin{Vmatrix} \lambda_1 & & & * \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{Vmatrix}$$

con raíces características $\lambda_1, \lambda_2, \ldots, \lambda_n$ en diagonal. Un análisis un poco más detallado termina con la reducción de A a una *forma normal de Jordan* $J(A)$ (véase el complemento), a una suma directa *de células de Jordan*

$$J_{m,\lambda} = \begin{Vmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & \lambda \end{Vmatrix}$$

($m \times m$ es la dimensión de la célula, λ es una de las raíces características).

Observemos, que si $A^q = E$, entonces, $J^q_{m,\lambda} = E_m$ es la $m \times m$-matriz unidad para cada célula de Jordan $J_{m,\lambda}$ de la matriz A, y esto, evidentemente, sólo es posible cuando $m = 1$ y λ es la raíz de grado q de 1 (como siempre, consideramos $K = \mathbb{C}$). En conse-

cuencia,

$$A^q = E \Rightarrow CAC^{-1} = \begin{Vmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{Vmatrix}, \quad \lambda_i^q = 1, \qquad (3)$$

para cierta matriz invertible C. Lo mismo se deduce de un criterio más simple de diagonalización del operador lineal $\mathcal{A}$ con la matriz A y el polinomio característico $f_A(t) = t^q - 1$ sin raíces múltiples.

Todos estos razonamientos, referidos a un operador aislado $\mathcal{A}$: $V \to V$, es útil tenerlos en cuenta al pasar al grupo $\Phi(g)$, $g \in G$, de operadores lineales.

DEFINICION 3. Sea (Φ, V) una representación lineal del grupo G. El subespacio $U \subset V$ se llama *invariante* (o *estable*) *respecto a* G, si $\Phi(g)\, u \in U$ para todo $u \in U$ y $g \in G$. El subespacio nulo y el propio espacio V de la representación Φ son subespacios invariantes *triviales*. La representación que sólo posee subespacios invariantes triviales, se denomina *irreducible*. La representación *es reducible*, si tiene por lo menos un subespacio invariante no trivial.

Conforme a lo dicho más arriba, en caso de una representación reducible (Φ, V) con subespacio invariante U, el espacio V tiene una base, con relacion a la cual

$$\Phi_g = \begin{Vmatrix} \Phi'_g & \Phi^0_g \\ 0 & \Phi''_g \end{Vmatrix} \qquad (4)$$

para todo $g \in G$. Como $\Phi'_{gh} = \Phi'_g \Phi'_h$, $\Phi'_e = E_k$ y $\Phi'_g(U) \subset U$, entonces, la aplicación Φ': $g \mapsto \Phi'_g$ define la representación en U, llamada *subrepresentación* en Φ. En el espacio cociente V/U también está definida la representación. Ella se llama *representación cociente* y es dada por las matrices Φ''_g, $g \in G$.

Si en V se puede elegir la base de tal modo que todas las matrices Φ^0_g sean nulas, entonces, se habla de una representación *descomponible* Φ, y más exactamente, sobre una *suma directa de representaciones* $\Phi = \Phi' + \Phi''$. La descomposición de (Φ, V) en una suma directa es realizable exactamente cuando el subespacio invariable $U \subset V$ tiene un subespacio invariante *suplementario* W, así que $V = U \oplus W$ es la descomposición en una suma directa de los subespacios, y $\Phi(U) \subset U$, $\Phi(W) \subset W$. Si esto es así, entonces, $\Phi' = \Phi|_U$, $\Phi'' = \Phi|_W$ son limitaciones de Φ en U y W respectivamente.

La representación lineal (Φ, V) se llama *indescomponible*, si no puede ser expresada en forma de suma directa de dos subrepresenta-

ciones no triviales. También se habla sobre el *G-espacio V indescomponible*.

Desintegrando sucesivamente, si esto es posible, V, U, W, etc., en la suma directa de subespacios invariantes, llegamos a la suma directa $V = V_1 \oplus \ldots \oplus V_r$ de varios subespacios invariantes (correspondientemente a la suma directa $\Phi = \Phi^{(1)} + \ldots \times \Phi^{(r)}$ de varias representaciones). Para una elección correspondiente de la base en V, las matrices de operaciones lineales toman la forma

$$\Phi_g = \begin{Vmatrix} \Phi_g^{(1)} & 0 & \ldots & 0 \\ 0 & \Phi_g^{(2)} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \Phi_g^{(r)} \end{Vmatrix}.$$

DEFINICION 4. La representación lineal (Φ, V) del grupo G, que es la suma directa de representaciones irreducibles, se denomina *completamente reducible*. Una terminología análoga se usa con respecto a los G-espacios.

Es intuitivamente claro que las representaciones irreducibles desempeñan el papel de bloques de construcción, de los cuales se construyen representaciones lineales arbitrarias. Las representaciones totalmente reducibles se obtienen como resultado del uso de la estructura elemental, la suma directa. En adelante se verá que en muchos casos esto es suficiente para describir todas las representaciones. Observemos que algunos grupos importantes para la física, como el de Lorentz, tienen *representaciones irreducibles de dimensiones infinitas*. Naturalmente, ellos no se reducen de ningún modo a los de dimensiones finitas y deben estudiarse por separado.

2. Ejemplos de representaciones lineales. Hemos dado todos los conceptos esenciales de la teoría de representaciones. Queda por llenarlos con contenido real, para lo que, al principio, es muy útil conocer (y entender fundamentalmente) la serie de ejemplos que se brindan a continuación.

EJEMPLO 1. El grupo lineal completo GL (n, K) sobre el campo K tiene, por definición, una representación lineal irreducible exacta de grado n con espacio de representación $V = K^n$. En este mismo espacio opera un grupo lineal cualquiera $H \supset$ GL (n, K) exacto, pero, posiblemente, reducible.

Observaciones análogas se refieren a otros grupos clásicos, indicados en el § 1 del cap. 7. Digamos, el grupo unidad $U(n)$ opera de un modo irreducible en el espacio hermítico, y el ortogonal, $O(n)$ en el euclídeo. Esto se deduce inmediatamente de la afirmación más fuerte, demostrada en el curso de álgebra lineal, que los grupos $U(n)$ y $O(n)$ operan transitivamente (en el sentido de ejemplo 3 del p. 3, § 2, cap 7) en el conjunto de vectores de longitud unitaria.

EJEMPLO 2. Haciendo operar a GL (n, K) en el espacio vectorial $M_n(K)$ de matrices de orden n por la regla ψ_A: $X \longmapsto AX$ $(A \in$ GL (n, K), $X \in M_n(K))$, nos convencemos fácilmente de que $\psi_A(\alpha X + \beta Y) = \alpha\psi_A X + \beta\psi_A Y$ y $\psi_{AB} = \psi_A\psi_B$. Por eso, $(\psi, M_n(K))$ es una relación lineal de grado n^2. Sea $M_n^{(i)}(K)$

un subespacio de las matrices

$$\begin{Vmatrix} 0 & \dots & x_{1i} & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & & x_{ni} & \dots & 0 \end{Vmatrix}$$

con una sola columna $X^{(i)}$ diferente de cero. Como es fácil comprobar, este subespacio es invariante respecto a Ψ_A, $A \in GL(n, K)$, irreducible e isomorfo (como el $GL(n, K)$ — espacio) al espacio natural K^n, en el cual opera $GL(n, K)$. De esto modo,

$$M_n(K) = M_n^{(1)}(K) \oplus \dots \oplus M_n^{(n)}(K)$$

es la descomposición en la suma directa de n $GL(n, k)$ — subespacios isomorfos, a lo que corresponde la descomposición

$$\Psi = \Psi^{(1)} + \dots + \Psi^{(n)}$$

en la suma directa de n representaciones equivalentes. Simbólicamente, este hecho se indica en forma

$$M_n(K) \cong nM_n^{(1)}(K); \quad \Psi \approx n\Psi^{(1)}$$

EJEMPLO 3. Definamos ahora la operación Φ del grupo $GL(n, K)$ en $M_n(K)$ haciendo $\Phi_A : X \mapsto AXA^{-1}$. Nuevamente, $(\Phi, M_n(K))$ es una representación lineal de grado n^2. Si $X = (x_{ij})$, entonces, como de costumbre, $\operatorname{tr} X = \sum_{i=1}^{n} x_{ii}$ es la traza de la matriz X. Es bien sabido que $\operatorname{tr}(\alpha X + \beta Y) = \alpha \operatorname{tr} X + \beta \operatorname{tr} Y$ (linealidad de la función tr) y $\operatorname{tr} \Phi_A(X) = \operatorname{tr} X$. De esto se deduce que el conjunto $M_n^0(k)$ de matrices con traza nula es un subespacio invariante respecto a Φ. Por otra parte, $\Phi_A(\lambda E) = \lambda E$ y $\operatorname{tr} \lambda E = n\lambda$. Así, en caso de un campo K de característica nula tiene lugar la descomposición en la suma directa de $GL(n, K)$ — subespacios

$$M_n(K) = \langle E \rangle \oplus M_n^0(K) \tag{5}$$

de dimensiones 1 y $n^2 - 1$ respectivamente. Notemos que cuando $n = p$ y $K = Z_p$ la descomposición del tipo (5) está ausente, por cuanto, en este caso, $\operatorname{tr} E = 0$.

De acuerdo con la definición, la forma normal de Jordan $J(X)$ de la matriz X no es otra cosa que la representación más sencilla y cómoda de $GL(n, \mathbb{C})$ — órbita, contenedora de X. La limitación de Φ en cualquier subgrupo $H \subset GL(n, K)$ hace natural la cuestión sobre los representantes canónicos de H-órbitas.

EJEMPLO 4. En el ejemplo anterior hagamos $K = \mathbb{R}$ y limitemos Φ en el grupo ortogonal $O(n)$. Como $A \in O(n) \iff {}^tA = A^{-1}$, entonces ${}^tX = \varepsilon X$, $\varepsilon = \pm 1$, ${}^t(AXA^{-1}) = {}^tA^{-1} \cdot {}^tX \cdot {}^tA = \varepsilon AXA^{-1}$. Por lo tanto, el espacio de la representación $M_n(\mathbb{R})$ del grupo $O(n)$ se escribe en forma de la suma de $O(n)$ — subespacios

$$M_n(\mathbb{R}) = \langle E \rangle_{\mathbb{R}} \oplus M_n^+(\mathbb{R}) \oplus M_n^-(\mathbb{R})$$

del espacio unidimensional $\langle E \rangle_{\mathbb{R}}$ de matrices escalares, del espacio $(n + 2) \times (n - 1)/2$-dimensional de matrices simétricas con traza nula y del espacio $n(n - 1)/2$-dimensional de matrices antisimétricas. Es bien conocida la correspondencia biunívoca entre las matrices simétricas (antisimétricas) y las formas bilineales simétricas (respectivamente, antisimétricas). La operación de $O(n)$ en $\langle E \rangle_{\mathbb{R}} \oplus M_n^+(\mathbb{R})$ y en $M_n^-(\mathbb{R})$ se traslada a los espacios de las formas correspondientes. El teorema sobre la reducción de la forma cuadrática $q(x)$ a los ejes principales, no es otra cosa, que la posibilidad de elección en la $O(n)$—

órbita, contenedora de $q(x)$, de la forma diagonal $\sum_j \lambda_i x_i$ con λ_i reales, determinados unívocamente con exactitud hasta la permutación.

Sustituyendo $\mathbb{R}$ por $\mathbb{C}$ y $O(n)$ por el grupo unidad $U(n)$, llegamos a la descomposición

$$M_n(\mathbb{C}) = \langle E \rangle_{\mathbb{C}} \oplus M_n^+(\mathbb{C}) \oplus M_n^-(\mathbb{C})$$

en la suma directa de $U(n)$—subespacios escalares, hermíticos con traza nula y matrices antihermíticas. El caso $n = 2$ fue analizado detalladamente en el § 1, cap. 7.

EJEMPLO 5. Sea G un grupo de permutaciones, que opera en cierto conjunto Ω con un número de elementos $|\Omega| = n > 1$, o sea, $G \subset S_n$. El espacio vectorial

$$V = \langle e_i \mid i \in \Omega \rangle_K$$

sobre el campo K de característica nula con base numerada por los elementos del conjunto Ω, lo transformamos en G-espacio, haciendo

$$\Phi(g)\left(\sum_{i\in\Omega} \lambda_i e_i\right) = \sum_{i\in\Omega} \lambda_i \Phi(g) e_i = \sum_{i\in\Omega} \lambda_i e_{g(i)}$$

($i \mapsto g(i)$ es la operación de permutación $g \in G$ en $i \in \Omega$). Como $(gh)(i) = g(h(i))$, entonces, se obtiene una representación lineal de grado n del grupo G. Ella nunca es irreducible, por cuanto

$$V = \left\langle \sum_{i\in\Omega} e_i \right\rangle \oplus \left\{ \sum_{\lambda_1+\ldots+\lambda_n=0} \lambda_i e_i \mid \lambda_i \in K \right\} \qquad (6)$$

es la descomposición en la suma directa de los espacios invariantes unidimensional y $(n-1)$-dimensional (si char $k = p > 0$ y $p \mid n$, entonces, ya no se obtiene una suma directa).

Separemos dos casos particulares.

a) $G + S_n$. El monomorfismo $S_n \to \mathrm{GL}(n, \mathbb{R})$, construido en el p. 5, § 3, cap. 4, coincide con nuestra representación lineal Φ, si se toma en calidad de e_i la i-ésima columna coordenada $E^{(i)}$. La descomposición (6) muestra que para S_n existe una inclusión más económica $S_n \to \mathrm{GL}(n-1, \mathbb{Q})$. Más tarde será demostrada la irreducibilidad de esta representación lineal de grado $n - 1$ (incluso sobre el campo $\mathbb{C}$).

b) *Representación regular*. Sea G un grupo finito cualquiera. Haciendo $\Omega = G$, obtendremos el llamado G-espacio regular $V = \langle e_g \mid g \in G \rangle$, y, correspondientemente, la *representación regular* (ρ, V) del grupo G: $\rho(a) e_g = e_{ag}$, para todo $a, g \in G$. Con la representación regular con designaciones algo distintas, ya nos encontramos al demostrar el teorema de Cayley (§ 3, cap. 4), pero, entonces no nos interesaba el espacio V, sino el conjunto $\{e_g\}$ de sus vectores básicos. El significado de la representación regular del grupo finito G consiste en que ella contiene todas las representaciones irreducibles de G, considerada con exactitud hasta la equivalencia (véase el § 5).

EJEMPLO 6. La representación de grado 1 es sencillamente el homomorfismo $\Phi: G \to K^*$ del grupo G en el grupo multiplicativo del campo K (K es un espacio vectorial unidimensional sobre sí mismo). Como el grupo multiplicativo de un campo es abeliano, entonces, $\mathrm{Ker}\, \Phi \supset G'$, donde G' es el conmutante del grupo G (teorema 4, § 3, cap. 7). Observemos que la *equivalencia de dos representaciones unidimensionales* Φ', Φ'' (con igual espacio de representación) es equivalente a la coincidencia de ambos, puesto que $a\Phi'(g)a^{-1} = \Phi''(g) \Rightarrow \Phi'(g) = \Phi''(g) \Rightarrow \Phi' = \Phi''$. Sea $g^n = e$. Entonces, $\Phi(g)^n = \Phi(g^n) = \Phi(e) = 1$, o sea, $\Phi(g)$ es raíz de la unidad. El núcleo de cualquier representación unidimensional puede ser no trivial incluso para el grupo cíclico G. Si, por ejemplo, $G = Z_4$ y $K = Z_{13}$, entonces, $\mathrm{Ker}\, \Phi \supset 2Z_4$. Por otra parte

en el caso en que $K = \mathbb{C}$, cualquier grupo cíclico tiene representación unidimensional exacta.

a) $G = (\mathbb{Z}, +)$. La representación $k \longmapsto \lambda^k$ para $|\lambda| \neq 1$ es exacta. Si $|\lambda| = 1$, entonces, según la fórmula de Euler, $\lambda = e^{2\pi i\theta}$, $\theta \in \mathbb{R}$, y el núcleo de la aplicación $k \longmapsto e^{2\pi i\theta k}$ es distinto de cero sólo cuando $\theta \in \mathbb{Q}$.

El grupo $\mathbb{Z}$ tiene representaciones complejas indescomponibles de grado tan grande como se quiera, que, sin embargo, no son irreducibles. Es suficiente apoyarse en el teorema sobre la forma normal de Jordan de una matriz y examinar la aplicación

$$k \longmapsto J^k_{m,1} = \left\| \begin{matrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{matrix} \right\|^k$$

b) $G = \langle a \mid a^n = e \rangle$. Sea $\varepsilon = e^{\frac{2\pi i}{n}}$ la raíz primitiva de grado n de 1. De n representaciones unidimensionales

$$\Phi^{(m)}: a^k \longmapsto \varepsilon^{mk}, \quad m = 0, \quad 1, \dots, n-1, \qquad (7)$$

$\varphi(n)$ serán exactas. Señalemos un hecho interesante: *el grupo cíclico de orden n tiene exactamente n representaciones irreducibles no equivalentes de dos en dos, sobre $\mathbb{C}$. Todas ellas son unidimensionales y tienen la forma* (7).

Efectivamente, sólo es necesario convencerse de que en un grupo cíclico finito no existen representaciones de dimensión > 1, irreducibles sobre $\mathbb{C}$. Pero, antes de la definición 3, se observó el hecho de que cualquier operador lineal $\Phi(g)$ de orden finito puede ser diagonalizado sobre $\mathbb{C}$. En este caso, ésto equivale a la reducibilidad total de la representación Φ. *Si* $\dim \Phi = r$, *entonces*, Φ *se descompone en la suma directa de m representaciones unidimensionales.*

Para el grupo cíclico de orden finito se ha obtenido, en esencia, la descripción de todas las representaciones lineales complejas. Con exactitud hasta la equivalencia

$$\Phi_g = \left\| \begin{matrix} \Phi_g^{(i_1)} & & 0 \\ & \ddots & \\ 0 & & \Phi_g^{(i_r)} \end{matrix} \right\|$$

donde $\Phi^{(m)}$ es una de las representaciones del tipo (7).

Nuestra finalidad consiste en establecer leyes semejantes en el caso general.

EJEMPLO 7. Ya en los ejemplos anteriores se estableció una fuerte dependencia de las propiedades de la representación lineal Φ del grupo G, respecto al campo fundamental K. Pongamos complementariamente en claro esta cuestión.

El grupo cíclico $G = \langle a \mid a^p = e \rangle$ de simple orden p, que opera en el espacio vectorial bidimensional $V = \langle v_1, v_2 \rangle$ sobre un campo arbitrario K de característica p, de acuerdo a la regla $a * v_1 = v_1$, $a * v_2 = v_1 + v_2$, define la representación *indescomponible* (Φ, V)

$$a^k \longmapsto \Phi_a^k = \left\| \begin{matrix} 1 & k \\ 0 & 1 \end{matrix} \right\|, \quad 0 \leqslant k \leqslant p-1.$$

En efecto, la matriz Φ_a tiene la raíz característica 1 de multiplicidad 2. Por eso, la descomposición de Φ en la suma directa de dos representaciones unidimensionales, significaría la existencia de la matriz invertible C, para la cual $C\Phi_aC^{-1} = \left\| \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \right\| = E$. Pero entonces, $\Phi_a = C^{-1}EC = E$, lo que no es cierto.

Sea luego, $G = \langle a \mid a^3 = e\rangle$ un grupo cíclico de orden 3 y $K = \mathbb{R}$. La representación bidimensional (Φ, V), $V = \langle v_1, v_2\rangle$, dada en la base prefijada por la matriz

$$\Phi_a = \begin{Vmatrix} -1 & -1 \\ 1 & 0 \end{Vmatrix},$$

es irreducible, por cuanto el polinomio característico $t^2 + t + 1$ de esta matriz no tiene raíces reales. Pero, si V se considera sobre $\mathbb{C}$, entonces, naturalmente, V se descompone en la suma directa de G-subespacios unidimensionales

$$V = \langle v_1 + \varepsilon^{-1} v_2\rangle \oplus \langle v_1 + \varepsilon v_2\rangle$$

$$C\Phi_a C^{-1} = \begin{Vmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{Vmatrix}, \qquad \varepsilon = \frac{-1+\sqrt{-3}}{2}, \qquad C = \begin{Vmatrix} 1 & -\varepsilon^{-1} \\ 1 & -\varepsilon \end{Vmatrix}.$$

De este modo, cuando se amplía el campo, la propiedad de irreducibilidad de la representación puede perderse.

En adelante, salvo raras excepciones, el campo fundamental K será el campo de los números complejos (el más importante desde el punto de vista práctico), o cualquier campo algebraico cerrado de característica nula.

EJERCICIOS

1. El grupo SO(2) se da mediante su representación bidimensional natural

$$\Phi'(\theta) = \begin{Vmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{Vmatrix},$$

irreducible sobre $\mathbb{R}$. Comprobar, que

$$A\Phi'(\theta)A = \begin{Vmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{Vmatrix} \quad \text{para } A = \frac{1}{\sqrt{2}} \begin{Vmatrix} 1 & i \\ i & 1 \end{Vmatrix} \in \mathrm{GL}(2, \mathbb{C}).$$

En consecuencia, Φ' es la suma directa de dos representaciones unidimensionales no equivalentes (en este caso, sencillamente distintas).

2. ¿Es o no irreducible el GL $(n, \mathbb{C})$-espacio $M_n^\circ(\mathbb{C})$ en la descomposición (5) para $n = 2$ y 3? (Respuesta: sí)

3. Sean Φ y Ψ representaciones complejas irreducibles del grupo cíclico $\langle a \mid a^n = e\rangle$ de orden n. Mostrar que

$$\frac{1}{n}\sum_{k=0}^{n-1} \Phi(a^k)\,\Psi(a^k) = \begin{cases} 1, & \text{si } \Phi \approx \Psi, \\ 0, & \text{si } \Phi \not\approx \Psi. \end{cases}$$

4. Apoyándose en el ejercicio 3, convencerse de la veracidad de la afirmación siguiente. Cualquier función compleja f en un grupo cíclico $\langle a \mid a^n = e\rangle$, se puede escribir en forma de una descomposición «por armónicos elementales»

$$f(a^k) = \sum_{m=0}^{n-1} c_m \varepsilon^{mk}, \quad \varepsilon = e.$$

Los «coeficientes de Fourier» c_m se calculan por medio de la fórmula

$$c_m = \frac{1}{n}\sum_{k=0}^{n-1} f(a^k)\,\varepsilon^{-mk}.$$

5. De la fórmula para el número de collares (véase el comienzo del capítulo) deducir las conclusiones elementales: a) $q^p - q \equiv 0 \pmod p$ (pequeño teorema de Fermat; véase el § 4, cap 4);

$$\text{b)} \sum_{d \mid n} \varphi(d) = n.$$

§ 2. UNITARIEDAD Y REDUCTIBILIDAD

1. Representaciones unitarias. Recordemos que, en el curso de álgebra lineal, la forma no degenerada $(u, v) \mapsto (u \mid v)$ en el espacio vectorial V sobre $\mathbb{C}$ se llama *hermítica*, si

$$(u \mid v) = \overline{(v \mid u)},$$
$$(\alpha u + \beta v \mid w) = \alpha (u \mid w) + \beta (v \mid w), \qquad (1)$$
$$(v \mid v) > 0 \text{ para todo } v \neq 0$$

(como siempre, $z \mapsto \bar{z}$ es el automorfismo de conjugación compleja). El espacio V, examinado junto con la forma hermítica no degenerada $(u \mid v)$, se llama espacio *hermítico*. El espacio *euclídeo* con productos escalares, dado por medio de la forma bilineal simétrica no degenerada, sirve de análogo del hermítico. Tomando la base $e_1, \ldots, e_n$ en V, escribamos la forma $(u \mid v)$ para $u = \sum u_i e_i$, $v = \sum v_j e_j$ del modo

$$(u|v) = \sum h_{ij} u_i \bar{v}_j.$$

La matriz $H = (h_{ij})$ cumple la condición $\bar{h}_{ij} = h_{ji}$ y también se llama *hermítica*. Ya empleamos esta terminología en el § 1, cap. 7.

Existe una base ortonormada (definida por la condición $(e_i \mid e_j) = \delta_{ij}$), con relación a la cual

$$(u|v) = \sum_{i=1}^{n} u_i \bar{v}_i.$$

El operador lineal $\mathcal{A}\colon V \to V$, que conserva esta forma, o sea, que posee la propiedad $(\mathcal{A}u \mid \mathcal{A}v) = (u \mid v)$, se llama operador *unitario*. En el caso real, a él le corresponde el operador *ortogonal*. La condición de unitariedad, escrita en forma matricial $A \cdot {}^t\bar{A} = E$ con $A = (a_{ij})$, ${}^t\bar{A} = A^* = (\bar{a}_{ji})$, ya la encontramos en el cap. 7. Designando por $\mathcal{A}^*$ el operador lineal con matriz ${}^t\bar{A} = A^*$, expresemos la condición de unitariedad en la forma $\mathcal{A} \cdot \mathcal{A}^* = \mathcal{E} = \mathcal{A}^* \cdot \mathcal{A}$.

El grupo de todas las matrices unitarias (grupo de operadores unitarios, o, simplemente, grupo unitario) se suele designar con el símbolo conocido $U(n)$. Por definición, $U(n) \subset \mathrm{GL}(n, \mathbb{C})$, *y si la representación* $\Phi\colon G \to \mathrm{GL}(n, \mathbb{C})$ *es tal, que* $\mathrm{Im}\,\Phi \subset U(n)$, *entonces*, (Φ, V) *se llama representación unitaria.*

TEOREMA 1. Toda representación lineal (Φ, V) sobre $\mathbb{C}$ *del grupo finito* G, *es equivalente a una representación unitaria.*

DEMOSTRACIÓN. Elijamos en el espacio de la representación V del grupo G una forma hermítica no degenerada cualquiera $H\colon (u, v) \mapsto H(u, v) = \sum h_{ij} u_i \bar{v}_j$ (la escritura es respecto a cierta base $f_1, \ldots, f_n$ del espacio V) y consideremos la forma $(u \mid v)$, obtenida de $H(u, v)$ «promediando» respecto a G:

$$(u|v) = |G|^{-1} \sum_{g \in G} H(\Phi(g)u, \Phi(g)v). \qquad (2)$$

El multiplicador $|G|^{-1}$ no es esencial y se puso sólo para que, en caso de ser H unitario, tuviese lugar la igualdad $(u \mid v) = H(u, v)$. Como

$$H(\Phi(g)u, \Phi(g)v) = \overline{H(\Phi(g)v, \Phi(g)u)},$$

$$H(\Phi(g)(\alpha u + \beta v), \Phi(g)w) =$$
$$= H(\alpha\Phi(g)u + \beta\Phi(g)v, \Phi(g)w) = \alpha H(\Phi g)u, \Phi(g)w) +$$
$$+ \beta H(\Phi(g)v, \Phi(g)w), \quad H(\Phi(g)v, \Phi(g)v) > 0$$

para $v \neq 0$ y todo $g \in G$, entonces, la forma (2) cumple la condición (1) y resulta, por consiguiente, una forma hermítica no degenerada.

Además (y esto es lo más importante),

$$(\Phi(g)u \mid \Phi(g)v) = |G|^{-1} \sum_{h\in G} H(\Phi(g)\Phi(h)u, \Phi(g)\Phi(h)v)$$
$$= |G|^{-1} \sum_{h\in G} H(\Phi(gh)u, \Phi(gh)v) =$$
$$= |G|^{-1} \sum_{t\in G} H(\Phi(t)u, \Phi(t)v) = (u \mid v)$$

o sea, el operador $\Phi(g)$ para cualquier $g \in G$ deja la forma $(u \mid v)$ invariante. Elijamos en V una base $e_1, \ldots, e_n$, ortonormada respecto a la forma $(u \mid v)$. Entonces, en esta base, las matrices Φ_g de los operadores $\Phi(g)$ serán unitarias. ∎

Observaciones. 1) La afirmación del teorema 1 no se deduce automáticamente del hecho por nosotros conocido, que cada matriz Φ_g con $g^m = e$, es semejante a la diagonal unitaria diag $\{\lambda_1, \ldots, \lambda_n\}$ con $\lambda_i^m = 1$.

2) En el caso real, un razonamiento totalmente análogo muestra, que la representación (Φ, V) es equivalente a la ortogonal.

3) Por muchas razones, las representaciones unitarias desempeñan un papel importante en las aplicaciones de la teoría de representaciones, y es muy notable, que el teorema 1 sigue siendo válido para una clase mucho más amplia de grupos compactos tales, como $U(n)$ y $O(n)$. La demostración es la misma, pero la suma por los elementos de los grupos se sustituye por integración (respecto a cierta medida) en el grupo. Recordemos, que el grupo compacto $SU(2)$ geométricamente no se diferencia de la esfera tridimensional S^3, y, por eso, tiene sentido hablar, por ejemplo, sobre su volumen. En general, existe un marcado paralelismo entre la teoría de representaciones y los grupos compactos, pero no tenemos posibilidad de detenernos en esto. Del ejemplo 6a) del § 1 se ve que las representaciones de grupos no compactos (por ejemplo, $G = \mathbb{Z}$) no son unitarias obligatoriamente.

Para finalizar, observemos, que aunque la demostración del teorema 1 es constructiva, no sería nada práctico utilizar en su búsqueda la realización unitaria de la representación que se tiene. Por ejemplo, para el grupo G engendrado por los elementos $a_1, \ldots, a_d$, es suficiente lograr la unitariedad de las matrices $\Phi a_1, \ldots, \Phi a_d$. Entonces, también el grupo $\langle \Phi a_1, \ldots, \Phi a_d \rangle = \Phi(G)$ será unitario.

EJEMPLO 1. El grupo simétrico $S_3 = \langle (12), (123) \rangle$ posee la representación bidimensional Φ, contenida en calidad de sumando directo en la representación tridimensional natural (véase el ejemplo 5 del § 1). Precisamente, si $\Phi(\pi)\, e_i = e_{\pi(i)}$, $i = 1, 2, 3$, y $f_1 = e_1 - e_3$, $f_2 = e_2 - e_3$, entonces,

$$\Phi((12))\, f_1 = e_2 - e_3 = f_2, \qquad \Phi((12))\, f_2 = e_1 - e_3 = f_1,$$
$$\Phi((123))\, f_1 = e_2 - e_1 = -f_1 + f_2, \qquad \Phi((123))\, f_2 = e_3 - e_1 = -f_1.$$

Como $\pi = (123)^i (12)^j$, donde $i = 0, 1$ ó 2 y $j = 0$ ó 1, entonces, sin esfuerzo se obtienen todas las matrices $\Psi_\pi = \Phi(\pi)_{(f_1, f_2)}$:

$$e \mapsto \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \quad (12) \mapsto \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}, \quad (13) \mapsto \begin{Vmatrix} -1 & -1 \\ 0 & 1 \end{Vmatrix}$$
$$(23) \mapsto \begin{Vmatrix} 1 & 0 \\ -1 & -1 \end{Vmatrix}, \quad (123) \mapsto \begin{Vmatrix} -1 & -1 \\ 1 & 0 \end{Vmatrix}, \quad (132) \mapsto \begin{Vmatrix} 0 & 1 \\ -1 & -1 \end{Vmatrix}.$$

De las relaciones $\det \begin{Vmatrix} -1 & -1 \\ 1 & 0 \end{Vmatrix} = 1$ y $(123)^3 = e$ se deriva que

$$C \begin{Vmatrix} -1 & -1 \\ 1 & 0 \end{Vmatrix} C^{-1} = \begin{Vmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{Vmatrix}, \quad \varepsilon = \frac{-1+\sqrt{-3}}{2},$$

para cierta matriz no degenerada C. La conjugación con ayuda de C no debe infringir la propiedad de unitariedad de la matriz

$$\begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}.$$

Las condiciones lineales

$$C \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix} C, \quad C \begin{Vmatrix} -1 & -1 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{Vmatrix} C, \quad C = \begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix}$$

son cumplidas por la matriz

$$C = \begin{Vmatrix} 1 & -\varepsilon^2 \\ -\varepsilon^2 & 1 \end{Vmatrix}.$$

Ahora tenemos la posibilidad de escribir las conocidas representaciones unitarias del grupo S_3: la unitaria $\Phi^{(1)}$, $\Phi^{(2)}$: $\pi \mapsto \operatorname{sgn}(\pi) = \pm 1$, y la representación bidimensional recién obtenida $\Phi^{(3)} \approx \Psi$. Para referencias ulteriores es cómoda la tabla:

π	e	(12)	(13)	(23)	(123)	(132)
$\Phi^{(1)}$	1	1	1	1	1	1
$\Phi^{(2)}$	1	-1	-1	-1	1	1
$\Phi^{(3)}$	$\begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}$	$\begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}$	$\begin{Vmatrix} 0 & \varepsilon \\ \varepsilon^{-1} & 0 \end{Vmatrix}$	$\begin{Vmatrix} 0 & \varepsilon^{-1} \\ \varepsilon & 0 \end{Vmatrix}$	$\begin{Vmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{Vmatrix}$	$\begin{Vmatrix} \varepsilon^{-1} & 0 \\ 0 & \varepsilon \end{Vmatrix}$

EJEMPLO 2. La representación ortogonal natural de un grupo infinito, precisamente del SU (2), obtiene el epimorfismo Φ: SU (2) $\mapsto$ SO (3), construido en el § 1, cap. 7.

2. Reductibilidad completa. De las definiciones y observaciones hechas en el § 1, es claro, en que medida resulta fundamental la afirmación siguiente.

TEOREMA 2 (teorema de Mashke). *Cada representación lineal del grupo finito G sobre el campo K de característica, no divisora de $|G|$ (en particular, nula), es completamente reducible.*

Recordemos, que la afirmación del teorema 2 significa la descomposición (Φ, V) en la suma directa de respresentantes irreducibles. Hablando con propiedad, el teorema clásico de Mashke dice lo siguiente.

(M) *Cada subespacio G-invariante $U \subset V$, posee el suplemento G-invariante W:*

$$V = U \oplus W. \tag{3}$$

Demostraremos, precisamente, esta afirmación, de la cual el teorema 2 se deduce automáticamente. En efecto, o la representación (Φ, V) es irreducible, y entonces no hay nada que demostrar, o bien existe su propio G-invariante subespacio U, y entonces es justa la descomposición (3) con cierto G-subespacio W. En este caso, $\dim U < \dim V$, $\dim W < \dim V$. Empleando los mismos razonamientos para U y W, y usando la inducción sobre la dimensión, obtenemos la descomposición requerida en componentes irreducibles. ∎

Pasamos a la demostración de la afirmación (M). Como antes, nos interesa más el caso del campo $K = \mathbb{C}$, por eso es útil traer dos razonamientos independientes.

PRIMERA DEMOSTRACION ($K = \mathbb{C}$). Conforme al teorema 1, existe una forma hermítica no degenerada $(u \mid v)$ en el espacio de la representación V, invariante respecto a los operadores lineales $\Phi(g)$. Para cada subespacio $U \subset V$ existe el *suplemento ortogonal*

$$U^{\perp} = \{v \in V \mid (u \mid v) = 0, \quad \forall\, u \in U\},$$

y por el conocido teorema del curso de álgebra lineal

$$V = U \oplus U^{\perp},$$

además, $(U^{\perp})^{\perp} = U$. Supongamos ahora, que U es un G-subespacio en V, o sea, $\Phi(g)\, U \subset U$ para todo $g \in G$. Como $\Phi(g)|_U$ es un automorfismo, entonces, cualquier elemento $u \in U$ se escribe en la forma $u = \Phi(g)\, u'$, $u' \in U$. Queda por aprovechar la invariancia de la forma

$$v \in U^{\perp} \Rightarrow (u \mid \Phi(g)\, v) = (\Phi(g)\, u' \mid \Phi(g)\, v) = (u' \mid v) = 0.$$

Por lo tanto, $v \in U^{\perp} \Rightarrow \Phi(g)\, v \in U^{\perp}$. Haciendo $W = U^{\perp}$, llegaremos a la descomposición (3). ∎

SEGUNDA DEMOSTRACION. Sea, como antes, U un subespacio en V, invariante respecto a la operación de G. Examinemos la suma directa

$$V = U \oplus U',$$

donde U' es un suplemento a U elegido arbitrariamente. Hablando en general, U' no es G-invariante. Consideremos el operador de proyección $\mathcal{P}$: $V \to U'$, definido por la relación

$$\mathcal{P}v = u'$$

para todo vector $v = u + u'$. Tenemos

$$v - \mathcal{P}v \in U, \quad \mathcal{P}(U) = 0, \quad \mathcal{P}^2 = \mathcal{P}. \tag{4}$$

Introduzcamos ahora el operador lineal «promediado»

$$\mathcal{P}_G = |G|^{-1} \sum_{h \in G} \Phi(h)\, \mathcal{P}\, \Phi(h^{-1})$$

(la división por $|G|$ es posible, por condición). Tenemos

$$\Phi(g)\, \mathcal{P}_G = \mathcal{P}_G\, \Phi(g), \quad \forall g \in G. \tag{5}$$

Efectivamente,

$$\Phi(g)\, \mathcal{P}_G \Phi(g^{-1}) = |G|^{-1} \sum_{h \in G} \Phi(g)\, \Phi(h)\, \mathcal{P}\Phi(h^{-1})\Phi(g^{-1}) =$$

$$= |G|^{-1} \sum_{h \in G} \Phi(gh)\, \mathcal{P}\Phi((gh)^{-1}) = |G|^{-1} \sum_{t \in G} \Phi(t)\, \mathcal{P}\Phi(t^{-1}) = \mathcal{P}_G,$$

que lleva a la relación (5). Hagamos

$$W = \mathcal{P}_G(V) = \{\mathcal{P}_G v \mid v \in V\}.$$

De acuerdo con (5), $\Phi(g)\, w = \Phi(g)\, \mathcal{P}_G v = \mathcal{P}_G \Phi(g)\, v = \mathcal{P}_G v' = w' \in W$, para todo $w \in W$, así que el subespacio vectorial $W \subset V$ realmente resulta un G-subespacio.

Queda demostrar, que $V = U \oplus W$ es la suma directa de G-subespacios. Como $\Phi(h^{-1})\, v - \mathcal{P}\Phi(h^{-1})\, v \in U$ (véase (4)), entonces, $v - \Phi(h)\, \mathcal{P}\, \Phi(h^{-1})\, v = \Phi(h)\, \{\Phi(h^{-1})\, v - \mathcal{P}\Phi(h^{-1}) \times v\} \in \Phi(h)\, U = U$ (invariancia de U). Por consiguiente,

$$v - \mathcal{P}_G v = |G|^{-1} \sum_{h \in G} (v - \Phi(h)\, \mathcal{P}\Phi(h^{-1})) = u \in U,$$

y obtenemos $v = u + w$, con $w = \mathcal{P}_G v \in W$, o sea, $V = U + W$.

Luego, $\Phi(h^{-1})\, U \subset U \Rightarrow \mathcal{P}\Phi(h^{-1})\, U = 0$ (véase (4)) $\Rightarrow \Phi(h) \times \mathcal{P}\Phi(h^{-1})\, U = 0 \Rightarrow \mathcal{P}_G(U) = 0$. Por lo tanto, $v - \mathcal{P}_G v = u \in U \Rightarrow \mathcal{P}_G(v - \mathcal{P}_G v) = 0$, de donde, $\mathcal{P}_G v = \mathcal{P}_G^2 v$ para todo $v \in V$. Esto significa que $\mathcal{P}_G$ es una proyección en W a lo largo de U:

$$\mathcal{P}_G(U) = 0, \quad \mathcal{P}_G^2 = \mathcal{P}_G. \tag{6}$$

Ahora $v \in U \cap W \Rightarrow \mathcal{P}_G\, v = 0$, por cuanto, $v \in U$, y $v = \mathcal{P}_G v'$, por cuanto $v \in \mathcal{P}_G(V) = W$. Usando (6), obtenemos $0 = \mathcal{P}_G\, v = \mathcal{P}_G(\mathcal{P}_G v') = \mathcal{P}_G^2 v' = \mathcal{P}_G v' = v \Rightarrow U \cap W = 0$. ∎

No es oportuno formular una conclusión más contundente acerca de la univocidad de la descomposición en componentes irreducibles (G-subespacios irreducibles): $V = V_1 \oplus V_2 \oplus \ldots \oplus V_r$. Si, por

ejemplo, $\Phi(g) = \mathscr{E}$ es un operador unidad para todo $g \in G$, entonces, cualquier descomposición directa de V en subespacios unidimensionales, será una descomposición en componentes irreducibles, y tales descomponentes son infinitamente muchas. Distinto es, si agrupamos todos los componentes irreducibles isomorfos:

$$V = U_1 \oplus \ldots \oplus U_s.$$

Como no distinguimos los G-espacios isomorfos, entonces, puede considerarse

$$U_1 = V_1 \oplus V_1 \oplus \ldots \oplus V_1 = n_1 V_1,$$
$$\ldots\ldots\ldots$$
$$U_s = V_s \oplus V_s \oplus \ldots \oplus V_s = n_s V_s,$$

donde n_i es la *multiplicidad de conformación* del componente irreducible V_i en la descomposición V. Veremos, que la multiplicidad se determina unívocamente.

EJERCICIOS

1. Toda representación continua unidimensional del grupo $(\mathbb{R}, +)$ (cuando a los números cercanos les corresponden operadores cercanos) tiene la forma $\Phi^{(\alpha)}: t \mapsto e^{i\alpha t}$, donde α es un número complejo. Mostrar que $\Phi^{(\alpha)}$ es unitario si, y sólo si, $\alpha \in \mathbb{R}$. (*Indicación.* Derivar la igualdad $e^{i\alpha t}\overline{e^{i\alpha t}} = 1$ respecto a t, y hacer $t = 0$.)

2. El núcleo del homomorfismo $f: t \mapsto \begin{Vmatrix} \cos t & -\operatorname{sen} t \\ \operatorname{sen} t & \cos t \end{Vmatrix}$ del grupo $(\mathbb{R}, +)$ en SO (2), se compone de los números $t = 2\pi m$, $m \in \mathbb{Z}$. De este modo, SO (2) $\cong \mathbb{R}/2\pi\mathbb{Z}$ y a cada representación unitaria irreducible Φ (conforme a los resultados del § 4, ella es necesariamente unidimensional) del grupo SO (2) le corresponde la representación unitaria irreducible $\tilde{\Phi}: t + 2\pi m \mapsto \Phi(t)$, $0 \leqslant t < 2\pi$, del grupo $\mathbb{R}$, para el cual $\tilde{\Phi}(2\pi) = \Phi(0) = 1$. Deducir del ejercicio 1, que $\tilde{\Phi} = \Phi^{(n)}$, $n \in \mathbb{Z}$. En combinación con la observación 3) del p. 1, esto significa, que toda representación irreducible del grupo SO (2) tiene la forma $\Phi^{(n)}(t) = e^{int}$, $n \in \mathbb{Z}$. Comprobar, que

$$\frac{1}{2\pi}\int_0^{2\pi} e^{ikt}\cdot\overline{e^{ilt}}\,dt = \delta_{kl}$$

(comparar con la relación en el ejercicio 3 del § 1: el orden n se ha sustituido por el «volumen» 2π del grupo SO (2)). En el análisis, el sistema de funciones $\{e^{int}\}$ sirve de ejemplo clásico de sistema ortonormal completo de funciones periódicas (o de funciones en la circunferencia $S^1 \sim$ SO (2)). Con esto comienza la vasta teoría de series de Fourier.

3. Con ayuda del teorema de Mashke demostrar que cualquier representación bidimensional compleja exacta de un grupo finito no abeliano, es irreducible.

4. Sean $\Phi: G \to U(n)$, $\Psi: G \to U(n)$, representaciones irreducibles unitarias equivalentes del grupo finito G. Demostrar que existe una matriz unitaria U,

para la cual $U\Phi_g U^{-1} = \Psi_g$, $\forall g \in G$. (*Indicación*. Por condición, $C\Phi_g C^{-1} = \Psi_g$, para cierta matriz $C = (c_{ij}) \in \mathrm{GL}(n, \mathbb{C})$. La operación $A \mapsto A^* = {}^t\bar{A}$, aplicada a $C\Phi_g = \Psi_g C$, da $\Phi^{-1}_g C^* = C^*\Psi^{-1}_g$, de donde, $\Phi^{-1}_g C^* C = C^* C\Phi^{-1}_g$. Por el lema de Schur $C^*C = \lambda E$. Luego, $\lambda = \sum_{k=1}^{n} |c_{ki}|^2 = \mu\bar{\mu}$, $\mu \in \mathbb{C}$, y $U = \mu^{-1}C$ es la matriz unitaria buscada.)

§ 3. GRUPOS FINITOS DE ROTACIONES

En este parágrafo se tratará sobre los subgrupos finitos del grupo SO (3). Conociéndolos, a un mismo tiempo obtendremos las representaciones ortogonales irreducibles de tales grupos, como A_4, S_4, A_5, además, en una envoltura geométrica fácilmente memorizable. En la primera lectura se puede omitir el punto 1 y la demostración (muy puntualizada) del teorema 2, pero, quien desee probar si ha asimilado bien la idea general de «operación de grupo» (§ 2, cap. 7), le será útil tomar conocimiento del contenido de todo el parágrafo.

1. Ordenes de los subgrupos finitos en SO(3). De acuerdo con el teorema de Euler del curso de álgebra lineal, todo elemento $\mathcal{A} \in \in \mathrm{SO}(3)$ $\mathcal{A} \neq \mathcal{E}$, es una rotación (giro) en el espacio euclídeo $\mathbb{R}^3$ alrededor de cierto eje. Con otras palabras, se tienen exactamente dos puntos en la esfera bidimensional unidad S^2, que permanecen inmóviles para una operación de $\mathcal{A}$: los puntos de intersección de la esfera con el eje de rotación. Estos dos puntos se llaman *polos de rotación de* $\mathcal{A}$.

Sean ahora, G un subgrupo finito en SO (3), y S el conjunto de polos de todas las rotaciones no unidades de G. Es claro, que G opera como grupo de permutaciones en el conjunto S. Si x es un polo para cierta rotación $\mathcal{A} \neq \mathcal{E}$, $\mathcal{A} \in G$, entonces, para cualquier $\mathcal{B} \in G$, tenemos

$$(\mathcal{B}\mathcal{A}\mathcal{B}^{-1})\,\mathcal{B}x = \mathcal{B}\cdot\mathcal{A}x = \mathcal{B}x,$$

o sea, $\mathcal{B}x$ es polo para $\mathcal{B}\mathcal{A}\mathcal{B}^{-1}$ y, por lo tanto, $\mathcal{B}x \in S$. Designemos con Ω el conjunto de todos los pares ordenados $(\mathcal{A}, x)$, donde $\mathcal{A} \in G$, $\mathcal{A} \neq \mathcal{E}$, x es polo para $\mathcal{A}$. Sea, luego, G_x el subgrupo estacionario (estabilizador) del punto x, o sea, el subgrupo en G de todos los elementos que dejan x en su lugar. Si

$$G = G_x \cup g_2 C_x \cup \ldots \cup g_{m_x} G_x$$

es la descomposición de G en clases adjuntas por la izquierda, respecto a G_x, entonces, la G-órbita del punto x será el conjunto

$$G(x) = \{x, g_2 x, \ldots, g_{m_x} x\}$$

con un número de elementos $|G(x)| = m_x$. Según el teorema de Lagrange, $N = m_x n_x$, donde $N = |G|$, $n_x = |G_x|$ (en compara-

ción con el § 1, cap. 7, las notaciones se han modificado un poco). Observemos, que n_x es el orden de un subgrupo cíclico en G, en el que cada uno de sus elementos es la rotación alrededor del eje que pasa por x. Se dice, que n_x es la *multiplicidad del polo* x, o que x es el n_x-*polo*.

A cada elemento $\mathcal{A} \neq \mathcal{E}$ de G le corresponden dos polos, por eso, $|\Omega| = 2(N-1)$.

Por otra parte, para cada polo x se tienen $n_x - 1$ elementos de G, distintos de e, que dejan inmóvil el polo x. Por consiguiente, el número de pares $(\mathcal{A}, x)$ es igual a la suma

$$|\Omega| = \sum_{x \in S} (n_x - 1).$$

Tomando como $\{x_1, \ldots, x_k\}$ el conjunto de polos, uno de cada órbita, haciendo $n_i = n_{x_i}$, $m_i = m_{x_i}$ y observando que $n_x = n_{x_i} = n_i$ para todo $x \in G(x_i)$, obtenemos

$$|\Omega| = \sum_{x \in S} (n_x - 1) = \sum_{i=1}^{k} m_i (n_i - 1) = \sum_{i=1}^{k} (N - m_i).$$

De este modo,

$$2N - 2 = \sum_{i=1}^{k} (N - m_i).$$

Dividiendo ambos miembros de la igualdad por N, tendremos

$$2 - \frac{2}{N} = \sum_{i=1}^{k} \left(1 - \frac{1}{n_i}\right). \tag{1}$$

Suponemos $N > 1$, así que $1 \leqslant 2 - \frac{2}{N} < 2$. Como $n_i \geqslant 2$, entonces, $\frac{1}{2} \leqslant 1 - \frac{1}{n_i} < 1$, y, por eso, k debe ser igual a 2 ó 3.

CASO 1. $k = 2$. Entonces

$$2 - \frac{2}{N} = \left(1 - \frac{1}{n_1}\right) + \left(1 - \frac{1}{n_2}\right),$$

o, lo que es equivalente,

$$2 = \frac{N}{n_1} + \frac{N}{n_2} = m_1 + m_2,$$

de donde, $m_1 = m_2 = 1$, $n_1 = n_2 = N$. Por lo tanto, G tiene exactamente un eje de rotación y $G = G_N$ es un grupo cíclico de orden N.

CASO 2. $k = 3$. Sea, para precisión, $n_1 \leqslant n_2 \leqslant n_3$. Si $n_1 \geqslant 3$, entonces, tendríamos

$$\sum_{i=1}^{3} \left(1 - \frac{1}{n_i}\right) \geqslant \sum_{i=1}^{3} \left(1 - \frac{1}{3}\right) = 2,$$

lo que es imposible. Por lo tanto, $n_1 = 2$, y la ecuación (1) se escribe en la forma

$$\frac{1}{2}+\frac{2}{N}=\frac{1}{n_2}+\frac{1}{n_3}.$$

Evidentemente, $n_2 \geqslant 4 \Rightarrow \frac{1}{n_2}+\frac{1}{n_3} \leqslant \frac{1}{2}$, es una contradicción. Por eso, $n_2 = 2$ ó 3.

Si $n_2 = 2$, entonces, $n_3 = \frac{N}{2} = m$ (N deberá ser par) y $m_1 = m_2 = m$, $m_3 = 2$. Estos datos corresponden al grupo del diedro D_m (véase el ejemplo 1, p. 5, § 3, cap. 7).

Si $n_2 = 3$, entonces

$$\frac{1}{6}+\frac{2}{N}=\frac{1}{n_3},$$

y tenemos sólo tres posibilidades:

2′) $n_3 = 3$, $N = 12$, $m_1 = 6$, $m_2 = 4$, $m_3 = 4$;
2″) $n_3 = 4$, $N = 24$, $m_1 = 12$, $m_2 = 8$, $m_3 = 6$;
2‴) $n_3 = 5$, $N = 60$, $m_1 = 30$, $m_2 = 20$, $m_3 = 12$.

Recojamos todos estos datos en la tabla:

N	números de órbitas	$\lvert S \rvert$	Órdenes de los estabilizadores		
n	2	2	n	n	—
$2m$	3	$2m+2$	2	2	m
12	3	14	2	3	3
24	3	26	2	3	4
60	3	62	2	3	5

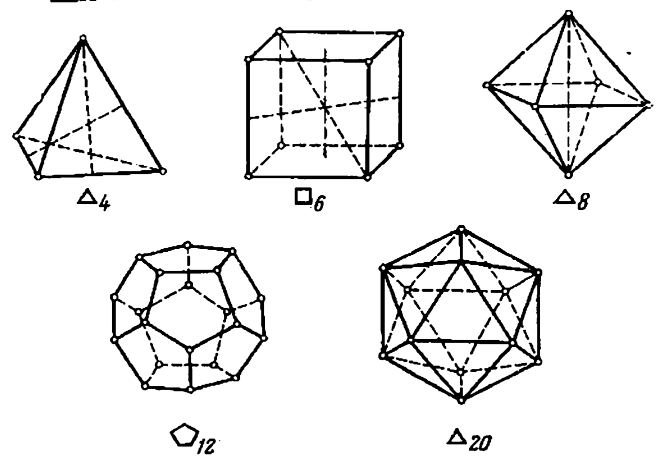
(2)

Hemos demostrado la afirmación siguiente.

TEOREMA 1. *Sea G un subgrupo finito en* SO (3), *ni diedral ni cíclico. Entonces, para su orden N se tienen solamente tres posibilidades*: $N = 12, 24$ *ó* 60. *Otras limitaciones al grupo G se hallan contenidas en la tabla* (2). ■

2. Grupos de poliedros regulares. La existencia de grupos de órdenes 12, 24 y 60, comprendidos en SO (3), se demuestra muy fácilmente. Con exactitud hasta la semejanza, existen sólo cinco (conocidos desde la antigüedad) poliedros regulares convexos en el espacio euclídeo $\mathbb{R}^3$: el tetraedro $\triangle_4$, el cubo $\square_6$, el octaedro $\triangle_8$, el dode-

caedro $⬠_{12}$ y el icosaedro $\triangle_{20}$:



Si el centro del poliedro regular M se coloca en el punto de origen del espacio $\mathbb{R}^3$, entonces, las rotaciones de SO (3) que hacen coincidir a M consigo, formarán un subgrupo finito. Pero, sin embargo, aparecen no cinco, sino sólo tres grupos de rotaciones diferentes (= no isomorfos), por cuanto para el cubo y el octaedro, y también para el dodecaedro e icosaedro, son iguales. Esto es muy fácil de explicar geométricamente. Si se unen con segmentos los puntos medios de las caras adyacentes del cubo, entonces, todos estos segmentos serán aristas del octaedro inscripto en el cubo. Cualquier rotación en $\mathbb{R}^3$, que deje el cubo invariante, traslada en sí mismo el octaedro inscripto y viceversa. Una observación igual es válida para el par dodecaedro — icosaedro. En la tabla a continuación N_0 es el número de vértices del poliedro, N_1 el número de aristas, N_2 el número de caras, μ es el número de aristas (lados) de cada cara, y ν el número de caras que convergen en cada vértice. Como antes, N es el orden del grupo correspondiente.

	N_0	N_1	N_2	μ	ν	N
Tetraedro . . . . . $\triangle_4$	4	6	4	3	3	12
Cubo . . . . $\square_6$	8	12	6	4	3	24
Octaedro . . . . . . $\triangle_8$	6	12	8	3	4	24
Dodecaedro . . . . . $⬠_{12}$	20	30	12	5	3	60
Icosaedro . . . . . . $\triangle_{20}$	12	30	20	3	5	60

De acuerdo con el teorema geométrico de Euler sobre los poliedros, $N_0 - N_1 + N_2 = 2$. El número total de polos es igual a $N_0 + N_1 + N_2 = 2N_1 + 2$. Para cualquier rotación que traslade al poliedro sobre sí mismo, una arista a_1b_1 dada coincide con cualquier otra a_ib_i o b_ia_i, de tal modo, que $N = 2N_1$. Observemos también, que $\{\mu, \nu\} = \{n_2, n_3\}$, donde n_2, n_3, son las multiplicidades de polos, formuladas en el p. 1.

Sean, luego, **T** el grupo del tetraedro; **O** el grupo del cubo (octaedro) e **I** el grupo del icosaedro (dodecaedro).

Los elementos de **T** son las rotaciones en ángulos alrededor de los cuatro ejes que unen los vértices con los centros de las caras opuestas, el giro en un ángulo π alrededor de cada uno de los tres ejes que unen los puntos medios de las aristas opuestas, y la rotación unidad.

En el grupo **O**, además de la rotación unidad, se tienen rotaciones en ángulos iguales a $\pi/2$, π, $3\pi/2$ alrededor de los tres ejes que unen los centros de las caras opuestas del cubo, rotaciones en ángulos $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ alrededor de cuatro ejes que unen los vértices opuestos extremos, y rotaciones en un ángulo π alrededor de cada uno de los seis ejes que unen los puntos medios de las aristas diagonalmente opuestas.

El tetraedro regular se inscribe en el cubo y queda invariante con respecto a algunas rotaciones de **O** de orden 3 y 2. Junto con la unidad son una cantidad de 12 tipos de rotaciones, y ellas componen, precisamente, el grupo **T**. En consecuencia, $\mathbf{T} \subset \mathbf{O}$, y como $|\mathbf{O} : \mathbf{T}| = 2$, entonces $\mathbf{T} \lhd \mathbf{O}$.

A cada elemento de **O** le corresponde exactamente una permutación en el conjunto, compuesto de las cuatro diagonales principales del cubo. De la igualdad de los órdenes de los grupos $|\mathbf{O}| = |S_4| = 24$, se deduce el isomorfismo de ellos: $\mathbf{O} \cong S_4$.

Respectivamente, $\mathbf{T} \cong A_4$.

El ejercicio 2 muestra que $\mathbf{I} \cong A_5$.

Volviendo a la demostración del teorema 1, observamos, que para $n_1 = 2$, $n_2 = n_3 = 3$, se tienen dos órbitas tetraelementales $G(p_1) = \{p_1, p_2, p_3, p_4\}$, $G(q_1) = \{q_1, q_2, q_3, q_4\}$ de los polos, donde p_i y q_i son puntos opuestos en la esfera S^2. Si $\triangle_4^\circ$ es un tetraedro con vértices p_i, entonces, su grupo de transformaciones de simetría $\mathbf{T}^\circ$ contiene a G. De $|G| = 12$ se deriva que $\triangle_4^\circ$ es un tetraedro regular, o sea, $\triangle_4^\circ = \triangle_4$ y $\mathbf{T}^\circ = G = \mathbf{T}$.

Para $n_2 = 3$, $n_3 = 4$, tomamos la órbita hexaelemental $G(p_1) = \{p_1, \ldots, p_6\}$ de los polos que se dividen en pares, por cuanto $i \neq 3 \Rightarrow n_i \neq 4$. Estos tres pares de puntos en la esfera S^2 los tomamos como tres pares de vértices opuestos del octaedro $\triangle_8^\circ$. Como en el caso anterior, $|G| = 24 \Rightarrow \triangle_8^\circ = \triangle_8$ (en el sentido que $\triangle_8^\circ$ es un octaedro regular) y $\mathbf{O}^\circ = G = \mathbf{O}$.

Finalmente, para $n_1 = 2$, $n_2 = 3$, $n_3 = 5$, se construye un

icosaedro $\triangle'_{20}$ con vértices p_i, tomados de las órbitas $G(p_1) = \{p_1, \ldots, p_{20}\}$. Nuevamente, $|G| = 60$, conlleva a la regularidad del icosaedro $\triangle^{\circ}_{20}$ y la coincidencia de los grupos: $\mathbf{I}^{\circ} = G = \mathbf{I}$.

Queda por observar, que cualesquiera dos poliedros regulares de un mismo tipo, inscriptos en la esfera S^2, se obtienen uno de otro mediante cierta rotación (cambio de sistema de coordenadas). Con esto se establece la conjugación de los subgrupos isomorfos en SO(3). Recojamos los resultados obtenidos, en forma de teorema.

TEOREMA 2. *Todos los subgrupos finitos en* SO(3) *se agotan, con exactitud hasta el isomorfismo, con los grupos* C_n, D_n, $n \in \mathbb{N}$; $\mathbf{T} \cong A_4$, $\mathbf{O} \cong S_4$ *e* $\mathbf{I} \cong A_5$. *Cualesquiera dos subgrupos finitos isomorfos son conjugados en* $SO(3)$. ∎

COROLARIO. *Los isomorfismos indicados en el teorema* 2, *dan representaciones ortogonales tridimensionales irreducibles de los grupos* A_4, S_4 *y* A_5. ∎

Empleando el teorema 2 y el epimorfismo Φ: SU(2) $\to$ SO(3) (teorema 1, § 1, cap. 7), llegamos fácilmente a la descripción de todos los subgrupos finitos del grupo SU(2) (se puede operar en el orden contrario). Cualquier grupo G^*, diferente del cíclico, resulta preimagen de cierto subgrupo finito $G \subset$ SO(3). Aparecen los llamados *grupos binarios*:

$$D_n^* = \Phi^{-1}(D_n), \quad \mathbf{T}^* = \Phi^{-1}(\mathbf{T}), \quad \mathbf{O}^* = \Phi^{-1}(\mathbf{O}), \quad \mathbf{I}^* = \Phi^{-1}(\mathbf{I}),$$

grupo binario del diedro, del tetraedro, del octaedro y del icosaedro. Los grupos binarios, al igual que las representaciones ortogonales Φ: SU(2) $\to$ SO(3) en general surgen naturalmente al describir los estados de sistemas físicos de partículas con spin.

EJERCICIOS

1. En el grupo $\mathbf{I}$ del icosaedro, además del subgrupo unidad, se tienen 15 subgrupos cíclicos conjugados de orden 2, 10 de orden 3, y 6 de orden 5. Demostrar, que $\mathbf{I}$ es un grupo simple. (*Indicación*. Mirar la demostración del teorema 5, § 3, cap. 7.)

2. Establecer el isomorfismo entre los grupos $\mathbf{I}$ y A_5. (*Indicación*. Utilizando la conjugación de todos los elementos de orden 2, mostrar, que ellos se disponen en «ramillete» (fig. 21) de cinco subgrupos de Sílov de orden 4 conjugados, disjuntos de dos en dos (más exactamente, intersecados respecto a e). El grupo $\mathbf{I}$ opera en el «ramillete» con conjugación. Esta operación es exacta, por cuanto $\mathbf{I}$ es un grupo simple (véase el ejercicio 1).)

3. Si H es un subgrupo finito de orden impar en SU (2) o SO (3), entonces, H es cíclico. (*Indicación*. Emplear el teorema sobre homomorfismos para el caso Φ: SU (2) $\to$ SO (3).)

4. Si el subgrupo finito $H \subset$ SU (2) no es preimagen de algún subgrupo $G \subset$ SO (3), entonces, $|H| \equiv 1$ (mód 2).

5. Mostrar, que con exactitud hasta la conjugación

$$D_3^* = \left\langle \left\| \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} \right\|, \left\| \begin{matrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{matrix} \right\| \middle| \varepsilon^2 + \varepsilon + 1 = 0 \right\rangle.$$

6. ¿Qué tienen de común entre sí el grupo binario I^* del icosaedro y el grupo

$$SL(2, Z_5) = \left\{ \left\| \begin{matrix} a & b \\ c & d \end{matrix} \right\| \,\middle|\, ad - bc - bc = 1;\ a, b, c, d \in Z_5 \right\} ?$$

7. Sea que los átomos q de diferentes calidades ($q < 200$) se disponen de todos los modos posibles (sin consideración de ninguna relación química) en los vértices del poliedro regular M. Las «moléculas» obtenidas unas de otras por

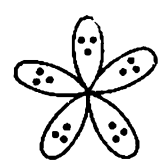


Fig. 22

rotación alrededor de cierto eje, no se diferencian. Sea $f(M, q)$ el número de «moléculas» distintas. Obtener las fórmulas:

$$f(\Delta_4, q) = \frac{q^2}{12}(q^2 + 11),$$

$$f(\square_6, q) = \frac{q^2}{24}(q^6 + 17q^2 + 6),$$

$$f(\Delta_8, q) = \frac{q^2}{24}(q^4 + 3q^2 + 12q + 8).$$

(*Indicación.* Usar los razonamientos empleados para el cálculo del número de collares (ejercicio 2, al principio del capítulo).)

8. Mostrar, que el cálculo del número de coloridos distintos de las caras M con pinturas de q calidades, conlleva, en el caso del tetraedro Δ_4 a la misma fórmula que en el ejercicio 7, y en el caso del cubo y del octaedro las fórmulas cambian de lugar.

§ 4. CARACTERES DE LAS REPRESENTACIONES LINEALES

1. Lema de Schur y su corolario. Toda teoría matemática interesante, habitualmente se basa en algunas ideas relativamente sencillas (pero afinadas). Una de las piedras de toque de la teoría de las representaciones, es la afirmación siguiente.

TEOREMA 1 (lema de Schur). *Sean* (Φ, V), (Ψ, W), *dos representaciones complejas irreducibles del grupo* G y $\sigma: V \to W$ *una aplicación lineal tal, que*

$$\Psi(g)\,\sigma = \sigma\Phi(g), \quad \forall g \in G. \tag{1}$$

Entonces:

(i) *si las representaciones* Φ, Ψ, *no son equivalentes, entonces* $\sigma = 0$;

(ii) *si* $V = W$, $\Phi = \Psi$, *entonces* $\sigma = \lambda\mathcal{E}$.

DEMOSTRACIÓN. Cuando $\sigma = 0$ no hay nada que demostrar. Por eso, consideramos $\sigma \neq 0$ y hacemos $V_0 = \operatorname{Ker}\sigma \subset V$.

Como $\sigma\Phi(g)v_0 = \Psi(g)\sigma v_0 = 0$, para cualquier $v_0 \in V_0$, entonces, $\Phi(g)V_0 = V_0$, o sea, el subespacio V_0 es invariante respecto a G. En virtud de la irreducibilidad de (Φ, V), tenemos $V_0 = 0$, o $V_0 = V$. La igualdad $V_0 = V$ es imposible, por cuanto $\sigma \neq 0$. Por lo tanto, $\operatorname{Ker}\sigma = 0$.

Análogamente, suponiendo $W_1 = \operatorname{Im}\sigma \subset W$, tendremos $w_1 \in W_1 \Rightarrow \Psi(g)w_1 = \Psi(g)\sigma(v_1) = \sigma(\Phi(g)v_1) = w_1' \in W_1$, así que W_1 es subespacio invariante en W. Nuevamente $\sigma \neq 0 \Rightarrow W_1 \neq 0$, y, por cuanto (Ψ, W) es una representación irreducible, queda la única posibilidad $W_1 = W$.

(i) Como $\operatorname{Ker}\sigma = 0$, $\operatorname{Im}\sigma = W$, en consecuencia, $\sigma: V \to W$ es un isomorfismo, y la condición (1) no es otra cosa que la condición de equivalencia de las representaciones Φ, Ψ (véase el § 1, definición 2). La afirmación (i) ha sido demostrada.

(ii) Por condición, $\sigma: V \to V$ es un operador lineal en V. Sea λ uno de sus valores propios; él existe, por cuanto el campo fundamental $\mathbb{C}$ es algebraicamente cerrado. El operador lineal $\sigma_0 = \sigma - \lambda\mathscr{E}$ tiene núcleo no trivial (en él está contenido el vector propio) y cumple la igualdad $\Psi(g)\sigma_0 = \sigma_0\Phi(g)$. Por lo demostrado antes, $\sigma_0 = 0$, o sea, $\sigma = \lambda\mathscr{E}$. ∎

COROLARIO. *Sean (Φ, V), (Ψ, W), dos representaciones irreducibles sobre $\mathbb{C}$ del grupo finito G de orden $|G|$, y $\sigma: V \to W$, una aplicación lineal cualquiera. Entonces, la aplicación «promediada»*

$$\tilde{\sigma} = \frac{1}{|G|}\sum_{g\in G}\Psi(g)\sigma\Phi(g)^{-1}$$

tiene las propiedades siguientes:

(i) $\Phi \not\sim \Psi \Rightarrow \tilde{\sigma} = 0$;

(ii) $V = W,\ \Phi = \Psi \Rightarrow \tilde{\sigma} = \lambda\mathscr{E},\ \lambda = \dfrac{\operatorname{tr}\sigma}{\dim V}$.

DEMOSTRACION. Tenemos

$$\Psi(g)\tilde{\sigma}\Phi(g)^{-1} = |G|^{-1}\sum_{h\in G}\Psi(g)\Psi(h)\sigma\Phi(h)^{-1}\Phi(g)^{-1} =$$
$$= |G|^{-1}\sum_{h}\Psi(gh)\sigma\Phi(gh)^{-1} = |G|^{-1}\sum_{t\in G}\Psi(t)\sigma\Phi(t)^{-1} = \tilde{\sigma},$$

así que $\Psi(g)\tilde{\sigma} = \tilde{\sigma}\Phi(g)$, $\forall g \in G$. Según el lema de Schur, inmediatamente se obtienen ambas afirmaciones, además, la precisión referida a la constante λ, se deduce de las relaciones

$$(\dim V)\lambda = \operatorname{tr}\lambda\mathscr{E} = \operatorname{tr}\tilde{\sigma} = |G|^{-1}\sum_{g\in G}\operatorname{tr}\Phi(g)\sigma\Phi(g)^{-1} =$$
$$= |G|^{-1}\sum_{g\in G}\operatorname{tr}\sigma = \operatorname{tr}\sigma.$$

Aquí hemos aprovechado la conocida propiedad de la función de la traza: $\operatorname{tr} CAC^{-1} = \operatorname{tr} A$. ■

Nos será necesaria la *formulación matricial del corolario*. Con este fin, elegimos en los espacios V, W, dos bases cualesquiera: $V = \langle e_i \mid i \in I \rangle$, $W = \langle f_j \mid j \in J \rangle$. Escribamos en estas bases nuestras aplicaciones (identificándolas con las matrices correspondientes):

$$\Phi_g = (\varphi_{ii'}(g)), \quad \Psi_g = (\psi_{jj'}(g)),$$
$$\sigma = (\sigma_{ji}), \qquad \tilde{\sigma} = (\tilde{\sigma}_{ji});\ i, i' \in I,\ j, j' \in J.$$

De acuerdo con la definición de $\tilde{\sigma}$,

$$\tilde{\sigma}_{ji} = |G|^{-1} \sum_{g\in G,\ i'\in I,\ j'\in J} \psi_{jj'}(g)\, \sigma_{j'i'} \varphi_{i'i}(g^{-1}). \tag{2}$$

La aplicación $\sigma\colon V \to W$ es totalmente arbitraria. Podemos tomar

$$\sigma_{ji} = 0, \quad \forall\ (j, i) \neq (j_0, i_0); \quad \sigma_{j_0 i_0} = 1. \tag{3}$$

Entonces, a la afirmación (i) del corolario le responde la relación

$$|G|^{-1} \sum_{g\in G} \psi_{jj_0}(g) \cdot \varphi_{i_0 i}(g^{-1}) = 0,$$
$$\forall i,\ i_0,\ j,\ j_0 \tag{4}$$

(Φ y Ψ son representaciones no equivalentes).

Si ahora $V = W$ y $\Phi = \Psi$, entonces

$$\operatorname{tr} \sigma = \sum \sigma_{ii} = \sum_{i',\, j'} \delta_{j'i'} \sigma_{j'i'},$$

$$\tilde{\sigma} = \frac{\operatorname{tr} \sigma}{\dim V} \mathcal{E} \Rightarrow \tilde{\sigma}_{ji} = \delta_{ji} \frac{\operatorname{tr} \sigma}{\dim V} = \frac{\delta_{ji}}{\dim V} \sum_{i',\, j'} \delta_{j'i'} \sigma_{j'i'}.$$

Comparando la expresión obtenida con (2), obtenemos

$$|G|^{-1} \sum_{g\in G,\ i',\, j'} \varphi_{jj'}(g)\, \sigma_{j'i'} \varphi_{i'i}(g^{-1}) = \frac{1}{\dim V} \sum_{i',\, j'} \delta_{ji} \delta_{j'i'} \sigma_{j'i'},$$

de donde, en virtud de la arbitrariedad en la elección de σ (véase (3)), llegamos a la conclusión, que la afirmación (ii) de corolario responde a la relación

$$|G|^{-1} \sum_{g\in G} \varphi_{jj_0}(g)\, \varphi_{i_0 i}(g^{-1}) = \begin{cases} \dfrac{\delta_{ji}}{\dim V}, & \text{si} \quad j_0 = i_0, \\ 0 \text{ en caso contrario.} \end{cases} \tag{5}$$

En las relaciones (4) y (5) se encuentra toda la información que necesitamos. ■

2. Caracteres de las representaciones. Con cada representación lineal finitodimensional compleja (Φ, V) del grupo G, se vincula la función

$$\chi_\Phi : G \to \mathbb{C},$$

definida por la relación

$$\chi_\Phi(g) = \operatorname{tr}\Phi(g), \quad g \in G,$$

y llamada *carácter de la representación*. Ella también se designa con el símbolo χ_V, o sencillamente con χ, si está claro de qué representación se trata.

Sea $\Phi_g = (\varphi_{ij}(g))$ la matriz que corresponde al operador $\Phi(g)$ en cierta base del espacio V, y $\lambda_1, \ldots, \lambda_n$ ($n = \dim V$) sus raíces características, tomadas teniendo en cuenta sus multiplicidades.

Por definición,

$$\chi_\Phi(g) = \chi_V(g) = \sum_{i=1}^{n} \varphi_{ii}(g) = \sum_{i=1}^{n} \lambda_i.$$

Si C es una matriz invertible cualquiera, entonces

$$\operatorname{tr} C\Phi_g C^{-1} = \operatorname{tr}\Phi_g.$$

Pero sabemos, que toda representación Ψ, equivalente a Φ, tiene la forma $g \mapsto C\Phi_g C^{-1}$. Por eso, *los caracteres de las representaciones isomorfas (equivalentes) coinciden*. Esta observación muestra, que el concepto de carácter está definido correctamente.

Señalemos otra serie de propiedades elementales de los caracteres.

PROPOSICIÓN. *Sea χ_Φ el carácter de una representación lineal compleja (Φ, V) del grupo G. Entonces:*

(i) $\chi_\Phi(e) = \dim V$;

(ii) $\chi_\Phi(hgh^{-1}) = \chi_\Phi(g)$, $\forall\, g, h \in G$, *o sea, χ_Φ es una función constante en las clases de elementos conjugados del grupo G;*

(iii) $\chi_\Phi(g^{-1}) = \overline{\chi_\Phi(g)}$, *para cualquier elemento $g \in G$ de orden finito (el sobrerayado indica conjugación compleja);*

(iv) *a la suma directa $\Phi = \Phi' + \Phi''$ de representaciones, le responde el carácter $\chi_\Phi = \chi_{\Phi'} + \chi_{\Phi''}$.*

DEMOSTRACIÓN. Efectivamente, $\chi_\Phi(e) = \operatorname{tr}\Phi(e) = \operatorname{tr}\mathcal{E} = \dim V$. Luego, $\chi_\Phi(hgh^{-1}) = \operatorname{tr}\Phi(hgh^{-1}) = \operatorname{tr}\Phi(h)\,\Phi(g)\,\Phi(h)^{-1} = \operatorname{tg}\Phi(g) = \chi_\Phi(g)$. Para la demostración de (iii) observemos, que

$$g^m = e \Rightarrow \Phi(g)^m = \mathcal{E}\,.$$

y si $\lambda_1, \ldots, \lambda_n$ son las raíces características del operador $\Phi(g)$, entonces, $\lambda_1^k, \ldots, \lambda_n^k$ serán las raíces características del operador $\Phi(g)^k$. En particular, $\lambda_i^m = 1$, $1 \leqslant i \leqslant n$, y, por lo tanto, $|\lambda_i| = 1$, $\overline{\lambda}_i = \lambda_i^{-1}$. Por eso

$$\chi_\Phi(g^{-1}) = \operatorname{tr}\Phi(g^{-1}) = \operatorname{tr2}\Phi(g)^{-1} = \sum_i \lambda_i^{-1} = \sum_i \overline{\lambda}_i = \overline{\left(\sum_i \lambda_i\right)} = \overline{\chi_\Phi(g)}.$$

Finalmente, en el caso $\Phi = \Phi' + \Phi''$ sabemos que con la correspondiente elección de la base en el espacio de la representación V, todas las matrices Φ_g, $g \in G$, adoptan la forma

$$\Phi_g = \begin{Vmatrix} \Phi'_g & 0 \\ 0 & \Phi''_g \end{Vmatrix},$$

de donde, $\operatorname{tr}\Phi_g = \operatorname{tr}\Phi'_g + \operatorname{tr}\Phi''_g$. Esto significa precisamente que $\chi_\Phi(g) = \chi_{\Phi'}(g) + \chi_{\Phi''}(g)$. ∎

Observemos, que para $n = \dim V = 1$ se tendrá $\chi_\Phi \in (g) = \Phi(g)$, pero, cuando $n > 1$, el carácter χ_Φ no es homomorfismo de G en $\mathbf{C}^*$.

EJEMPLO 1. Examinemos el grupo SU(2) en su representación bidimensional natural. Sea χ el carácter correspondiente. De acuerdo con (5), § 1, cap. 7, cualquier matriz $g \in SU(2)$ es conjugada con la matriz

$$b_\varphi = \begin{Vmatrix} e^{i\frac{\varphi}{2}} & 0 \\ 0 & e^{-i\frac{\varphi}{2}} \end{Vmatrix}, \quad 0 \leqslant \varphi < 2\pi,$$

así que las clases de elementos conjugados del grupo SU (2) se parametrizan con los números reales φ del intervalo indicado. En correspondencia con la propiedad (ii) de los caracteres, tenemos

$$\chi(g) = \chi(Ub_\varphi U^{-1}) = \chi(b_\varphi) = e^{i\frac{\varphi}{2}} + e^{-i\frac{\varphi}{2}} = 2\cos\frac{\varphi}{2}.$$

Con una representación canónica Φ: SU (2) → SO (3), la matriz b_φ pasa a la matriz

$$B_\varphi = \begin{Vmatrix} \cos\varphi & -\operatorname{sen}\varphi & 0 \\ \operatorname{sen}\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{Vmatrix},$$

que también sirve de cómodo representante en la clase de matrices ortogonales conjugadas del grupo SO (3). Es evidente, que

$$\chi_\Theta(B_\Phi) = 1 + 2\cos\varphi. \quad (6)$$

Usaremos la fórmula (6) más adelante.

El conjunto $\mathbf{C}^G = \{G \to \mathbf{C}\}$ de todas las funciones de G en $\mathbf{C}$ está dotado de estructura natural de espacio vectorial sobre $\mathbf{C}$: para $\alpha_1, \alpha_2 \in \mathbf{C}$, $\chi_1, \chi_2 \in \mathbf{C}^G$, bajo $\alpha_1\chi_1 + \alpha_2\chi_2$ se entiende la función con los valores

$$(\alpha_1\chi_1 + \alpha_2\chi_2)(g) = \alpha_1\chi_1(g) + \alpha_2\chi_2(g).$$

La función de $\mathbf{C}^G$ se llama *central*, si ella es constante respecto a las clases conjugadas del grupo G. Las funciones centrales generan, evidentemente, el espacio vectorial en $\mathbf{C}^G$, que designaremos con el símbolo $X_\mathbf{C}(G)$. Hablando en general, $X_\mathbf{C}(G)$ es un espacio infinitodimensional, pero, si en el grupo G sólo se tiene un número finito de clases de elementos conjugados $C_1, C_2, \ldots, C_r$ (así será siempre para el grupo finito G), entonces, el espacio $X_\mathbf{C}(G)$ es finitodimensional. Por ejemplo,

$$X_\mathbf{C}(G) = \langle \Gamma_1, \Gamma_2, \ldots, \Gamma_r \rangle_\mathbf{C}, \quad (7)$$

donde

$$\Gamma_i(g)=\begin{cases}1, & \text{si } g\in C_i,\\ 0, & \text{si } g\notin C_i.\end{cases}$$

Por lo demostrado (proposición (ii)), los caracteres del grupo G pertenecen al espacio $X_{\mathbf{C}}(G)$. Veremos, que el espacio estirado en ellos, de hecho coincide con $X_{\mathbf{C}}(G)$, por lo menos para el grupo finito G.

Más adelante suponemos, que el grupo G es finito. Transformemos $\mathbf{C}^G$ en espacio hermítico con el producto escalar

$$(\delta, \tau)_G=\frac{1}{|G|}\sum_{g\in G}\sigma(g)\overline{\tau(g)},\quad \sigma,\ \tau\in\mathbf{C}^G. \tag{8}$$

Es fácil comprobar, que la forma $(\sigma, \tau)\mapsto(\sigma, \tau)_G$ cumple todas las propiedades de una forma hermítica no degenerada. Su estrechamiento en el subespacio $X_{\mathbf{C}}(G)\subset\mathbf{C}^G$, resulta un instrumento muy útil, en particular para el estudio de los caracteres de las representaciones lineales.

TEOREMA 2. *Sean Φ, Ψ, representaciones complejas irreducibles del grupo finito G. Entonces,*

$$(\chi_\Phi, \chi_\Psi)_G=\begin{cases}1, & \text{si } \Phi\approx\Psi\\ 0, & \text{si } \Phi\not\approx\Psi.\end{cases} \tag{9}$$

DEMOSTRACION. En notaciones matriciales tenemos

$$\chi_\Phi(g)=\sum_{i=1}^{n}\varphi_{ii}(g),\quad \chi_\Psi(g)=\sum_{i=1}^{n}\psi_{ii}(g).$$

Haciendo $i_0=i$, $j_0=j$ en la relación (4), y sumando luego con respecto a i y j (en los intervalos admisibles para i y j), obtendremos

$$0=|G|^{-1}\sum_{g,i,j}\psi_{jj}(g)\varphi_{ii}(g^{-1})=|G|^{-1}\sum_{g}\Big(\sum_j\psi_{jj}(g)\Big)\Big(\sum_i\varphi_{ii}(g^{-1})\Big)=$$
$$=|G|^{-1}\sum_{g\in G}\chi_\Psi(g)\chi_\Phi(g^{-1})=|G|^{-1}\sum_{g\in G}\chi_\Psi(g)\overline{\chi_\Phi(g)}=(\chi_\Psi, \chi_\Phi)_G$$

para cualesquiera representaciones irreducibles no equivalentes Φ, Ψ, del grupo G.

Empleemos ahora (para $i_0=i$, $j_0=j$) la relación (5):

$$1=\Big(\sum_{i,j}\delta_{ji}\Big)/\dim V=|G|^{-1}\sum_{g\in G}\Big(\sum_j\varphi_{jj}(g)\Big)\Big(\sum_i\varphi_{ii}(g^{-1})\Big)=$$
$$=|G|^{-1}\sum_{g\in G}\chi_\Phi(g)\chi_\Phi(g^{-1})=(\chi_\Phi, \chi_\Phi)_G.$$

Como los caracteres de las representaciones isomorfas coinciden, entonces, $(\chi_\Phi, \chi_\Psi)_G = 1$, para $\Phi \approx \Psi$. ■

La expresión (9) se llama (primera) *relación de ortogonalidad* para los caracteres.

COROLARIO. *Sea*

$$V = V_1 \oplus \ldots \oplus V_k \qquad (10)$$

la descomposición del G-espacio V en la suma directa de G-subespacios irreducibles V_i. Si W es algún G-espacio irreducible con carácter χ_W, entonces, el número de sumandos V_i en (10), *isomorfos a W, es igual a $(\chi_V, \chi_W)_G$ y no depende del procedimiento de descomposición (multiplicidad con la que W entra en el G-espacio V). Dos representaciones (dos G-espacios) con el mismo carácter, son isomorfas.*

DEMOSTRACIÓN. Como mencionamos antes (proposición (iv)), $\chi_V = \chi_{V_1} + \ldots + \chi_{V_k}$, por eso

$$(\chi_V, \chi_W)_G = (\chi_{V_1}, \chi_W)_G + \ldots + (\chi_{V_k}, \chi_W)_G.$$

Según el teorema 2, en el segundo miembro se tiene una suma de k ceros y unidades, además, el número de unidades coincide con el de G-subespacios V_i, isomorfos a W. Pero el producto escalar $(\chi_V, \chi_W)_G$ en general, no depende de ninguna descomposición (véase la relación definitoria (8)), así que hemos demostrado simultáneamente la invarianza de la multiplicidad con la que W entra en el G-espacio V.

Dos G-espacios V, V', con el mismo carácter $\chi = \chi_V = \chi_{V'}$ contienen en su descomposición cualquier sumando, isomorfo al G-espacio dado irreducible W, el mismo número de veces, precisamente $(\chi, \chi_W)_G$. Por eso, en las descomposiciones

$$V = \bigoplus_{i=1}^{k} V_i, V' = \bigoplus_{j=1}^{l} V'_j$$

en sumandos directos irreducibles, podemos considerar $l = k$, $V'_i \cong V_i$, $1 \leqslant i \leqslant k$. Por consiguiente, también son isomorfos los mismos G-espacios V, V'. ■

Las observaciones hechas después de la demostración del teorema de Mashke y el corolario del teorema 2, permiten expresar el carácter χ_Φ de cualquier representación lineal compleja (Φ, V) de un grupo finito G, en forma de una combinación lineal de números enteros

$$\chi_\Phi = \sum_{i=1}^{s} m_i \chi_i.$$

Aquí, m_i es la multiplicidad, con la que la representación irreducible (Φ_i, V_i) entra en la descomposición (Φ, V), así que $\Phi_i \not\approx \Phi_j$, para $i \neq j$. Usando la relación de ortogonalidad (9), podemos escribir:

$$(\chi_\Phi, \chi_\Phi)_G = \sum_{i=1}^{s} m_i^2. \qquad (11)$$

Por lo tanto, el *cuadrado escalar* $(\chi_\Phi, \chi_\Phi)_G$ *de carácter* χ_Φ *de cualquier representación compleja* Φ, *siempre es un número entero, igual a 1 exactamente cuando* Φ *es una representación irreducible.* ▌

Llegamos a un resultado extraordinario. Los caracteres, o «trazas de las representaciones», portadores de referencias muy escasas sobre cada factor lineal $\Phi(g)$ por separado, expresan propiedades esenciales de la globalidad de éstos $\{\Phi(g) \mid g \in G\}$, o sea, de las propiedades de la propia representación Φ.

EJEMPLO 2. Convenzámonos de la irreducibilidad sobre $\mathbb{C}$ de las representaciones de los grupos A_4, S_4 y A_5 de rotaciones del espacio tridimensional. Para eso hay que regresar al corolario del teorema 2, § 3, y aprovecharse de las fórmulas (6) y (11). La representación Φ, descripta en el § 3 muestra que si π es una permutación de orden q, entonces, $\Phi(\pi)$ es un giro a un ángulo $k\frac{2\pi}{q}$, m.c.d. $(k, q) = 1$, alrededor de cierto eje. Por eso, el valor del carácter $\chi = \chi_\Phi$ se calcula inmediatamente por la fórmula (6):

$$\chi(\pi) = 1 + 2\cos k\frac{2\pi}{q} = 3,\ -1,\ 0,\ 1,\ \frac{1+\sqrt{5}}{2},\ \frac{1-\sqrt{5}}{2},$$

si, respectivamente, $q = 1, 2, 3, 4, 5$ $(k = \pm 1)$, 5 $(k = \pm 2)$. Observemos, que

$$\frac{1+\sqrt{5}}{2} = \operatorname{tr}\begin{Vmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon^{-1} & 0 \\ 0 & 0 & 1 \end{Vmatrix} = \varepsilon + \varepsilon^{-1} + 1,$$

$$\frac{1-\sqrt{5}}{2} = \varepsilon^2 + \varepsilon^{-2} + 1, \quad \varepsilon = e^{\frac{2\pi i}{5}}.$$

El cálculo del orden de la permutación π por su descomposición en ciclos independientes fue descripto en el corolario 1 del teorema 4, § 2, cap. 4. La distribución de los elementos respecto a las clases conjugadas viene dada en las tablas (para A_4 véase el ejercicio 8, § 2, cap. 7; para S_4 véase el ejercicio 4, § 3, cap. 7, y para A_5 véase la demostración del teorema 5, § 3, cap. 7). He aquí las mismas tablas, completadas con los valores del carácter χ:

	1	3	4	4
A_4	e	(12) (34)	(123)	(132)
χ	3	-1	0	0

S_4	1	3	6	8	6
	e	(12) (34)	(12)	(123)	(1234)
χ	3	—1	—1	0	1

A_5	1	15	20	12	12
	e	(12) (34)	(123)	(12345)	(12354)
χ	3	—1	0	$(1+\sqrt{5})/2$	$(1-\sqrt{5})/2$

Las relaciones

$$(\chi,\ \chi)_{A_4}=\frac{1}{12}\{1\cdot 3^2+3(-1)^2+4\cdot 0^2+4\cdot 0^2\}=1$$

$$(\chi,\ \chi)_{S_4}=\frac{1}{24}\{1\cdot 3^2+3(-1)^2+6(-1)^2+8\cdot 0^2+6\cdot 1^2\}=1,$$

$$(\chi,\ \chi)_{A_5}=\frac{1}{60}\Big\{1\cdot 3^2+15(-1)^2+20\cdot 0^2+$$

$$+12\left(\frac{1+\sqrt{5}}{2}\right)^2+12\left(\frac{1-\sqrt{5}}{2}\right)^2\Big\}=1$$

muestran, que la representación Φ con carácter χ es irreducible sobre $\mathbb{C}$ (véase (11)).

EJERCICIOS

1. Sean Φ, Ψ, representaciones complejas irreducibles del grupo finito G. Obtener la generalización del teorema 2:

$$|G|^{-1}\sum_{g}\chi_{\Psi}(hg)\,\overline{\chi_{\Phi}(g)}=\delta_{\Phi,\,\Psi}\,\frac{\chi_{\Phi}(h)}{\chi_{\Phi}(e)}\,.$$

Aquí h es un elemento arbitrario del grupo G: $\delta_{\Phi,\Psi}=1$ ó 0, según la equivalencia o no equivalencia de Φ y Ψ. (*Indicación*. Reescribir las relaciones (4) y (5) en la forma

$$|G|^{-1}\sum_{g}\psi_{jj_0}(g)\,\varphi_{i_0i}(g^{-1})=\delta_{\Phi,\,\Psi}\,\frac{\delta_{ji}\delta_{j_0i_0}}{\chi_{\Phi}(e)}\,.$$

Multiplicar ambos miembros por $\psi_{kj}(h)$ y sumar con respecto a j, tomando en cuenta la igualdad $\sum_j \psi_{kj}(h)\psi_{jj_0}(g) = \psi_{kj_0}(hg)$. En la relación obtenida

$$|G|^{-1}\sum_g \psi_{kj_0}(hg)\varphi_{j_0i}(g^{-1}) = \delta_{\Phi,\Psi}\frac{\psi_{ki}(h)\delta_{j_0i_0}}{\chi_\Phi(e)}$$

hacer $j_0 = k$, $i_0 = i$, y luego sumando con respecto a i y k, pasar a los caracteres.)

2. Emplear el criterio de irreductibilidad basado en los caracteres, en la representación $\Phi^{(3)}$ del grupo S_3 del ejemplo 1, punto 1, § 2.

3. Demostrar, con ayuda del lema de Schur, que todas las representaciones irreducibles sobre $\mathbb{C}$ del grupo abeliano G, son unidimensionales. (*Indicación.* Sean, Φ una representación irreducible; h un elemento de G. En virtud de la conmutatividad $\Phi(g)\Phi(h) = \Phi(h)\Phi(g)$, $\forall_g \in G$. Haciendo $\sigma = \Phi(h)$ en el lema de Schur, obtendremos $\Phi(h) = \lambda_h \mathscr{E}$. Esto es cierto para cualquier $h \in G$. Para una Φ irreducible queda la única posibilidad: ser unidimensional.)

4. Si el grupo G posee el automorfismo τ, entonces, con cada representación lineal (Φ, V) de este grupo, se asocia otra representación (Φ^τ, V), definida por la regla $\Phi^\tau(g) = \Phi(\tau(g))$. Comprobar, que esto es efectivamente así, y mostrar, que la irreducibilidad de Φ conlleva la irreducibilidad de Φ^τ. Por lo común, $\Phi^\tau \approx \Phi$, pero, en algunos casos, se obtiene una representación nueva. ¿Qué se puede esperar en caso de automorfismo interno?

Sean $G = A_5$ y Φ la representación examinada en el ejemplo 2. La aplicación τ: $\pi \mapsto (12)\pi(12)^{-1}$ es automorfismo (externo) del grupo A_5, que permuta las clases con representantes (12345) y (12354). El conjunto de valores de los caracteres χ y χ^τ se obtienen unos de otros por permutación de los lugares $(1+\sqrt{5})/2$ y $(1-\sqrt{5})/2$. Mostrar, que los caracteres χ y χ^τ no son equivalentes.

§ 5. REPRESENTACIONES IRREDUCIBLES DE GRUPOS FINITOS

1. Número de representaciones irreducibles. En caso de grupos finitos, las consideraciones precedentes permiten dar respuesta a las preguntas principales de la teoría de representaciones. Una de las fundamentales es el siguiente

TEOREMA 1. *El número de representaciones no equivalentes de dos en dos e irreducibles del grupo G sobre $\mathbb{C}$, es igual al número de sus clases de elementos conjugados.*

La demostración del teorema se contiene en los lemas 1 y 2, si se observa que la cantidad r de clases conjugadas del grupo G la interpretamos como la dimensión del espacio $X_{\mathbb{C}}(G)$ de las funciones centrales de signatura compleja en G (véase (7), § 4). Como los caracteres de las representaciones lineales son funciones centrales, entonces, ellos engendran en $X_{\mathbb{C}}(G)$ un espacio lineal de cierta dimensión $s \leqslant r$. Según el teorema 2, § 4, los caracteres de representaciones irreducibles conforman la base ortonormal (en métrica $(*, *)_G$) de este espacio. Por lo tanto, el número que nos interesa coincide con s y no es mayor que r. Queda por establecer la igualdad $s = r$.

LEMA 1. *Sean, Γ la función central en el grupo finito G, y (Φ, V) la representación irreducible sobre $\mathbb{C}$ con carácter χ_Φ. Entonces, para el operador lineal*

$$\Phi_\Gamma = \sum_{h\in G} \overline{\Gamma}(h)\,\Phi(h):\ V \to V$$

tenemos $\Phi_\Gamma = \lambda\mathscr{E}$, *donde*

$$\lambda = \frac{|G|}{\chi_\Phi(e)}\,(\chi_\Phi,\ \Gamma)_G$$

($\overline{\Gamma}$ *es una función central, definida por la igualdad* $\overline{\Gamma}(g) = \overline{\Gamma(g)}$).

DEMOSTRACION. Como Γ es una función central, entonces

$$\Phi(g)\,\Phi_\Gamma\Phi(g)^{-1} = \sum_{h\in G} \overline{\Gamma}(h)\,\Phi(g)\,\Phi(h)\,\Phi(g^{-1}) =$$

$$= \sum_{h\in G} \overline{\Gamma}(ghg^{-1})\,\Phi(ghg^{-1}) = \sum_{t\in G} \overline{\Gamma}(t)\,\Phi(t) = \Phi_\Gamma$$

Y bien, $\Phi_\Gamma\Phi(g) = \Phi(g)\,\Phi_\Gamma$, $\forall g \in G$. El lema de Schur (teorema 1, § 4), aplicado al caso $\sigma = \Phi_\Gamma$, muestra que $\Phi_\Gamma = \lambda\mathscr{E}$. Calculando la traza de los operadores que figuran en ambos miembros de esta igualdad, hallamos

$$\lambda\chi_\Phi(e) = \lambda \dim V = \operatorname{tr}\lambda\mathscr{E} = \operatorname{tr}\Phi_\Gamma = \sum_{h\in G} \overline{\Gamma}(h)\operatorname{tr}\Phi(h) =$$

$$= |G|\left\{|G|^{-1}\sum_{h\in G} \chi_\Phi(h)\,\overline{\Gamma(h)}\right\} = |G|\,(\chi_\Phi,\ \Gamma)_G. \blacksquare$$

LEMA 2. *Los caracteres $\chi_1, \ldots, \chi_s$ de todas las representaciones irreducibles no equivalentes de dos en dos del grupo G sobre $\mathbb{C}$ generan una base ortonormal del espacio $X_\mathbb{C}(G)$.*

DEMOSTRACIÓN. Por el teorema 2, § 4, el sistema $\chi_1, \ldots, \chi_s$ es ortonormal y se puede incluir en la base ortonormal del espacio $X_\mathbb{C}(G)$. Sea Γ una función central cualquiera, ortogonal con respecto a todo χ_i: $(\chi_i, \Gamma)_G = 0$. Entonces, según el lema 1, el operador lineal $\Phi_\Gamma^{(i)}$, que responde a la representación $\Phi^{(i)}$ con el carácter χ_i, es igual a cero.

Según el teorema de Mashke, toda representación compleja se puede descomponer en la suma directa

$$\Phi = m_1\Phi^{(1)} \dotplus \ldots \dotplus m_s\Phi^{(s)}$$

con algunas multiplicidades $m_1, \ldots, m_s$. En correspondencia con esta descomposición para el operador Φ_Γ, definido por la relación

$$\Phi_\Gamma = \sum_{h\in G} \overline{\Gamma}(h)\,\Phi(h),$$

tenemos

$$\Phi_\Gamma = m_1\Phi_\Gamma^{(1)} + \ldots m_s\Phi_\Gamma^{(s)} = 0.$$

En particular, esto se refiere al operador lineal ρ_Γ, donde ρ es una representación regular (véase el ejemplo 5, § 1). Pero en tal caso, tendremos (designando temporalmente con el símbolo 1 el elemento unidad del grupo G, a fin de evitar la combinación e_e)

$$0 = \rho_\Gamma (e_1) = \sum_{h \in G} \bar{\Gamma}(h)\, \rho(h)\, e_1 = \sum_{h \in G} \bar{\Gamma}(h)\, e_h \Rightarrow \bar{\Gamma}(h) = 0, \ \forall h\, G,$$

de donde $\bar{\Gamma} = 0$ y, en consecuencia, $\Gamma = 0$. ∎

EJEMPLO. El teorema 1, aplicado al grupo simétrico S_3, afirma, que este grupo tiene exactamente tres representaciones complejas irreducibles. No hace falta buscarlas: la tabla al final del p. 1, § 2, contiene toda la información necesaria. Notemos, de paso, que los cuadrados de los grados de las representaciones $\Phi^{(1)}$, $\Phi^{(2)}$, $\Phi^{(3)}$ satisfacen la relación $1^2 + 1^2 + 2^2 = 6 = |S_3|$. Ahora veremos, que en el caso general se cumple una relación análoga.

2. Grados de representaciones irreducibles. Examinemos un poco más detalladamente la representación regular $(\rho, \langle e_g \mid g \in G \rangle_\mathbb{C})$. Designemos mediante R_h la matriz del operador lineal $\rho(h)$ en la base dada $\{e_g \mid g \in G\}$. Como $\rho(h)\, e_g = e_{hg}$, entonces, todos los elementos diagonales de la matriz R_h serán nulos para $h \neq e$, y $\operatorname{tr} R_h = 0$. Por lo tanto.

$$\chi_\rho(e) = |G|, \quad \chi_\rho(h) = 0, \quad \forall h \neq e. \tag{1}$$

Sea ahora (Φ, V) una representación irreducible arbitraria del grupo G sobre $\mathbb{C}$. Como muestra el corolario del teorema 2, § 4, la multiplicidad de la inclusión de Φ en ρ es igual al producto escalar $(\chi_\rho, \chi_\Phi)_G$. De acuerdo con (1)

$$(\chi_\rho, \chi_\Phi)_G = |G|^{-1} \sum_{h \in G} \chi_\rho(h)\, \overline{\chi_\Phi(h)} = |G|^{-1} \chi_\rho(e)\, \overline{\chi_\Phi(e)} =$$
$$= |G|^{-1} |G|\, \chi_\Phi(e) = \dim V. \tag{2}$$

Vemos, que cada representación irreducible (considerada con exactitud hasta la equivalencia) entra en la regular con una multiplicidad igual a su grado. Según el teorema 1 se tienen r representaciones irreducibles no equivalentes de dos en dos

$$\Phi^{(1)}, \Phi^{(2)}, \ldots, \Phi^{(r)}$$

(r es el número de clases conjugadas del grupo G), a las cuales corresponden los caracteres

$$\chi_1, \chi_2, \ldots, \chi_r; \quad \chi_i = \chi_{\Phi^{(i)}},$$

de grados

$$n_1, n_2, \ldots, n_r; \quad n_i = \chi_i(e).$$

Habitualmente, como $\Phi^{(1)}$ se toma la representación unidad, así que $\chi_1(g) = 1$, $\forall g \in G$. La relación (2) muestra, que

$$\rho = n_1 \Phi^{(1)} + \ldots + n_r \Phi^{(r)},$$

de donde

$$\chi_\rho = n_1\chi_1 + \ldots + n_r\chi_r.$$

En particular,

$$|G| = \chi_\rho(e) = n_1\chi_1(e) + \ldots + n_r\chi_r(e) = n_1^2 + \ldots + n_r^2.$$

Llegamos al teorema siguiente.

TEOREMA 2. *Cada representación irreducible $\Phi^{(i)}$ entra en la descomposición de la representación regular ρ con una multiplicidad igual a su grado n_i. El orden $|G|$ del grupo finito G y los grados $n_1, \ldots, n_r$ de todas sus representaciones no equivalentes están vinculados por la relación*

$$\sum_{i=1}^{r} n_i^2 = |G|. \blacksquare \tag{3}$$

Para grupos de orden pequeño, la hermosa expresión (3) resulta suficiente para hallar todos los grados $n_1, \ldots, n_r$, aunque en el caso general es necesario, por supuesto, efectuar razonamientos complementarios.

Los datos sobre los caracteres de las representaciones irreducibles (más breve: sobre caracteres irreducibles) es cómodo escribirlos en forma de tabla

	e	g_2	g_3	$\ldots$	g_r
χ_1	n_1	$\chi_1(g_2)$	$\chi_1(g_3)$	$\ldots$	$\chi_1(g_r)$
χ_2	n_2	$\chi_2(g_2)$	$\chi_2(g_3)$	$\ldots$	$\chi_2(g_r)$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
χ_r	n_r	$\chi_r(g_2)$	$\chi_r(g_3)$	$\ldots$	$\chi_r(g_r)$

llamada *tabla de caracteres*. En su fila superior se encuentran los representantes de todas las r clases conjugadas g_i^G del grupo G. Por ejemplo, la tabla de caracteres del grupo S_3 tiene la forma

	e	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

(compararla con la tabla al final del p. 1 § 2).

Como siempre, designemos con el símbolo $C(g) = C_G(g)$ el centralizador en el grupo G del elemento $g \in G$. Sabemos, que $|C(g)|\,|g^G| = |G|$ (véase el punto 2, § 2, cap. 7). Por eso, la rela-

ción (9), § 4 (primera relación de ortogonalidad) se reescrita en la forma

$$\sum_{j=1}^{r} \frac{\chi_i(g_j)}{\sqrt{|C(g_j)|}} \overline{\frac{\chi_k(g_j)}{\sqrt{|C(g_j)|}}} = \frac{1}{|G|} \sum_{j=1}^{r} \frac{|G|}{|G(g_j)|} \chi_i(g_j) \overline{\chi_k(g_j)} =$$

$$= \frac{1}{|G|} \sum_{j=1}^{r} |g_j^G| \chi_i(g_j) \overline{\chi_k(g_j)} = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_k(g)} = (\chi_i, \chi_k)_G = \delta_{ik},$$

significa, que la $r \times r$-matriz

$$M = \left(\frac{\chi_i(g_j)}{\sqrt{|C(g_j)|}} \right)$$

es unitaria por filas. Pero la unitariedad por filas es equivalente a la unitariedad por columnas $(M \cdot {}^t\overline{M} = E = {}^t\overline{M} \cdot M)$, así que

$$\sum_{i} \frac{\chi_i(g_j)}{\sqrt{|C(g_j)|}} \overline{\frac{\chi_i(g_k)}{\sqrt{|C(g_k)|}}} = \delta_{jk},$$

o, en una escritura más detallada:

$$\sum_{i=1}^{r} \chi_i(g) \overline{\chi_i(h)} = \begin{cases} 0, & \text{si } g \text{ y } h \text{ no son conjugados,} \\ |C_G(g)|, & \text{en el caso contrario.} \end{cases} \blacksquare \tag{4}$$

La expresión (4) se llama *segunda relación de ortogonalidad* para los caracteres.

3. Representaciones de grupos abelianos. La descripción de las representaciones irreducibles de grupos cíclicos en el ejemplo 6, § 1, permite la generalización natural siguiente.

TEOREMA 3. *Cada representación irreducible de un grupo abeliano finito A sobre* **C** *es de grado* 1. *El número de tales representaciones no equivalentes de dos en dos es igual al orden de* $|A|$. *Recíprocamente, si cada representación irreducible del grupo A es de grado* 1, *entonces, A es un grupo abeliano.*

DEMOSTRACION. El número r de clases de elementos conjugados del grupo abeliano A coincide con el orden de éste, por eso, las dos primeras afirmaciones se deducen del teorema 2 (véase también el ejercicio 3, § 4). Haciendo, luego, en la relación (3) todos los n_i iguales a 1, obtendremos $r = |A|$, lo que es equivalente a la conmutatividad del grupo. $\blacksquare$

DEFINICION. Sea A un grupo abeliano. El conjunto

$$\hat{A} = \mathrm{Hom}\,(A, \mathbf{C}^*)$$

de homomorfismos de grupo A en el grupo multiplicativo $\mathbf{C}^*$ del campo de los números complejos, considerado junto con la operación corriente de multiplicación

$$(\chi_1\chi_2)(a) = \chi_1(a)\,\chi_2(a)$$

$(\chi_t \in \hat{A}, a \in A)$, se llama *grupo de caracteres* del grupo A sobre C $(\chi^{-1} = \overline{\chi})$.

TEOREMA 4. *Los grupos A y Â son isomorfos.*

DEMOSTRACION. Del teorema 3 sabemos, que, en todo caso $|A| = |\hat{A}|$. Conforme a los resultados del § 5 cap. 7, el grupo A permite la descomposición

$$A = A_1 \times A_2 \times \ldots \times A_k$$

en el producto directo de los grupos cíclicos $A_i = \langle a_i \rangle$ (no importa cuáles, primarios o no; elegimos la escritura multiplicativa de la ley de multiplicación en A). Si $|A_i| = s_i$ y ε_i es la raíz primitiva de s_i-ésimo grado de 1, entonces, a cada elemento $a = a_1^{t_1} a_2^{t_2} \ldots a_k^{t_k}$ de A, le corresponde el carácter $\chi_a \in \hat{A}$, definido por la relación

$$\chi_a (a_1^{r_1} a_2^{r_2} \ldots a_k^{r_k}) = \varepsilon_1^{r_1 t_1} \varepsilon_2^{r_2 t_2} \ldots \varepsilon_k^{r_k t_k}.$$

Evidentemente, $\chi_a \chi_{a'} = \chi_{aa'}$ (véase la definición). Si

$$a = a_1^{t_1} a_2^{t_2} \ldots a_k^{t_k} \neq a_1^{t'_1} a_2^{t'_2} \ldots a_k^{t'_k} = a',$$

entonces, existe un índice i con $t_i \neq t'_i$. En este caso,

$$\chi_a (a_i) = \varepsilon_i^{t_i} \neq \varepsilon_i^{t'_i} = \chi_{a'} (a_i).$$

Por consiguiente, todos los caracteres χ_a son diferentes de dos en dos y la aplicación $a \mapsto \chi_a$ establece el isomorfismo exigido entre A y $\hat{A}$. ∎

El método de demostración del teorema 4 brinda, evidentemente, una estructura clara de todas las representaciones irreducibles de un grupo abeliano.

EJEMPLO. Sean, V_{2^n} un grupo abeliano elemental de orden 2^n, χ su carácter complejo irreducible, distinto de la unidad, o sea, $\chi(a) \neq 1$ para algún $a \in V_{2^n}$. Entonces, Ker $\chi = B \cong V_{2^{n-1}}$ y tiene lugar la descomposición $V_{2^n} = B \cup aB$ en clases adjuntas respecto a B, así que

$$\chi (a^i b) = (-1)^i, \quad i = 0, 1.$$

En particular, el grupo cuaterno (de Klein) V_4, sobre las representaciones del cual se hizo mención en el problema 2, § 2, cap. 1, tiene la tabla de caracteres siguiente:

	e	a	b	ab
χ_1	1	1	1	1
χ_2	1	—1	1	—1
χ_3	1	1	—1	—1
χ_4	1	—1	—1	1

Los resultados sobre las representaciones de grupos abelianos, permiten obtener también cierta información acerca de las representaciones de grupos finitos arbitrarios.

TEOREMA 5. *Las representaciones de grado 1 del grupo finito G sobre $\mathbb{C}$ se encuentran en correspondencia biyectiva con las representaciones irreducibles del grupo cociente G/G' (G' es el conmutante del grupo G). El número de las mismas es igual al índice $(G : G')$.*

DEMOSTRACION. Hagamos primero una observación general. Sea, G un grupo cualquiera, y K su subgrupo normal. Si Φ es la representación del grupo G con núcleo $\operatorname{Ker}\Phi \supset K$, entonces, se puede definir la representación $\bar{\Phi}$ del grupo cociente G/K, suponiendo

$$\bar{\Phi}(gK) = \Phi(g), \quad g \in G.$$

Que esta definición es correcta, resulta evidente (véase la demostración del teorema 1, § 3, cap. 7). Luego, $\operatorname{Ker}\bar{\Phi} = \operatorname{Ker}\Phi/K$. En particular, para $K = \operatorname{Ker}\Phi$ se obtiene la representación exacta $\bar{\Phi}$.

Recíprocamente, toda representación lineal Ψ del grupo H, induce la representación Φ del grupo G, que permite el epimorfismo $\pi\colon G \twoheadrightarrow H$. Es suficiente hacer

$$\Phi(g) = \Psi(\pi(g)).$$

Como π es un epimorfismo, entonces, $\Phi(G) = \Psi(H)$ y Φ, Ψ, son al mismo tiempo reducibles o irreducibles. Según el teorema sobre la correspondencia (teorema 3, § 3, cap. 7) $\operatorname{Ker}\Phi = \pi^{-1}(\operatorname{Ker}\Psi)$. Con cualquier representación unidimensional Φ del grupo G se asocia el grupo abeliano (más exactamente, cíclico) $\operatorname{Im}\Phi$, así que $\operatorname{Ker}\Phi \supset G'$. La demostración del teorema se obtiene ahora como resultado de una sencilla unión del teorema 3, de la observación efectuada más arriba y del teorema 4, § 3, cap. 7. ∎

4. Representaciones de algunos grupos especiales. Aunque en principio, para la obtención de todas las representaciones irreducibles del grupo finito G, es suficiente descomponer su representación regular (teorema 2), en la práctica esto supone dificultades y se deben elegir rodeos. Habitualmente resulta más sencillo construir primero la tabla de caracteres, y luego formular las propias representaciones (véase, en relación con esto, el § 1, cap. 9). Por otra parte, en los ejemplos relativamente sencillos que se brindan más abajo, no hay ninguna necesidad de recurrir a diferentes subterfugios.

EJEMPLO 1. Sea G un grupo de permutaciones 2-transitivo arbitrario, que opera en el conjunto $\Omega = \{1, 2, \ldots, n\}$, $n > 2$ (véase el ejemplo 3, § 2, cap. 7). Sea, luego, Φ la representación natural del grupo G en el espacio $V = \langle e_1, e_2, \ldots, e_n\rangle$ con la operación $\Phi(g)\, e_i = e_{g(i)}$ (véase el ejemplo 5, § 1). Como es fácil comprender, el valor $\chi_\Phi(g)$ coincide con el número $N(g)$ de puntos $i \in \Omega$ (=a los vectores básicos e_i), que quedan inmóviles cuando opera g. Según el teorema 3, § 2, cap. 7, tenemos

$$\sum_{g\in G} \chi_\Phi(g)\,\overline{\chi_\Phi(g)} = \sum_{g\in G} \chi_\Phi(g)^2 \sum_{g\in G} N(g)^2 = 2\,|G|,$$

lo que, evidentemente, se reescribe en la forma

$$(\chi_\Phi, \chi_\Phi)_G = 2, \tag{5}$$

Comparando (5) con la relación (11) del § 4, llegamos a la conclusión de que Φ es la suma directa de dos representaciones irreducibles ($2 = 1 + 1$ es la única expresión de 2 en forma de suma de los cuadrados de números naturales). Pero, también sabemos, que $\Phi = \Phi^{(1)} + \Psi$, donde $(\Phi^{(1)}, U)$ es una representación unidad, y Ψ es una representación $(n-1)$-dimensional, que opera en el espacio $W = \langle e_1 - e_n, e_2 - e_n, \ldots, e_{n-1} - e_n \rangle$. Si la descomposición $V = U \oplus W$ se pudiese continuar a cuenta de la descomposición de W, entonces, los sumandos irreducibles serían más de dos. De este modo, tiene lugar la afirmación no trivial siguiente.

La representación lineal natural (Φ, V) *del grupo de permutaciones bitransitivo* G *sobre el campo* $\mathbb{C}$, *es la suma de la representación unidad más otra representación irreducible.* ∎

En particular, cada uno de los grupos S_n, $n > 2$; A_n, $n > 3$, *tiene una representación irreducible* Ψ *sobre* $\mathbb{C}$, *de grado* $n-1$, *con carácter* χ_Ψ, *y se calcula por la fórmula*

$$\chi_\Psi(g) = N(g) - 1. \quad ∎ \tag{6}$$

Como se mostró en el ejemplo del grupo S_3 (ejemplo 1, punto 1, § 2), las matrices Ψ_g se hallan fácilmente. Para el cálculo de los valores $\chi_\Psi(g)$ por la fórmula (6), es suficiente conocer la estructura cíclica de la permutación g.

Tenemos una breve ilustración:

A_4	e	(12)(34)	(123)	(132)
χ_Ψ	3	−1	0	0

S_4	e	(12)(34)	(12)	(123)	(1234)
χ_Ψ	3	−1	1	0	−1

A_5	e	(12)(34)	(123)	(12345)	(12354)
χ_Ψ	4	0	1	−1	−1

EJEMPLO 2. *Representaciones irreducibles del grupo alternativo* A_4. Recojamos los hechos que nos son conocidos. El grupo A_4 tiene cuatro clases de elementos conjugados. Los representantes de las clases y sus potencias se muestran en las dos filas superiores de la

tabla

	1	3	4	4
	e	(12)(34)	(123)	(132)
χ_1	1	1	1	1
χ_2	1	1	ε	ε^{-1}
χ_3	1	1	ε^{-1}	ε
χ_4	3	—1	0	0

El conmutante $A_4' = \{e, (12)(34), (13)(24), (14)(23)\} \cong V_4$ tiene índice 3 en A_4, por eso, A_4 posee tres representaciones unidimensionales $\Phi^{(1)} = \chi_1$, $\Phi^{(2)} = \chi_2$, $\Phi^{(3)} = \chi_3$ (con núcleo A_4' y con $\varepsilon^3 = 1$, $\varepsilon \neq 1$) y una representación tridimensional $\Phi^{(4)}$ ($12 = 1^2 + 1^2 + 1^2 + 3^2$). Comparando la tabla para A_4 del ejemplo 1 con la del ejemplo 2, § 4, nos convencemos de que la representación $\Phi^{(4)}$ con carácter χ_4 es equivalente a la representación Φ del grupo A_4 de rotaciones (grupo del tetraedro) y a la representación Ψ, vinculada con la 2-transitividad del grupo A_4.

EJEMPLO 3. *Representaciones irreducibles del grupo simétrico S_4.* Las dos filas superiores de la tabla

	1	3	6	8	6
	e	(12)(34)	(12)	(123)	(1234)
χ_1	1	1	1	1	1
χ_2	1	1	—1	1	—1
χ_3	2	2	0	—1	0
χ_4	3	—1	—1	0	1
χ_5	3	—1	1	0	—1

se han tomado del ejercicio 4, § 3, cap. 7. La representación $\Phi^{(1)} = \chi_1$ es unidad. La representación $\Phi^{(2)} = \chi_2$ se da mediante la paridad (con el signo) de permutaciones de S_4. Como $(S_4 : S_4') = 2$ (ejemplo del p. 2, § 3, cap. 7), entonces,no hay más representaciones unidimensionales. La representación bidimensional $\Phi^{(3)}$ con carácter χ_3 y núcleo $V_4 \lhd S_4$ se obtiene de los razonamientos expuestos en la demostración del teorema 5 y en el ejemplo 2, p. 1, § 3, cap. 7. La representación $\Phi^{(4)}$ con carácter χ_4 responde a las rotaciones del cubo (véase la tabla para S_4 del ejemplo 2, § 4). La representación $\Phi^{(5)} = \Psi$, con carácter χ_5 (véase la tabla en el ejemplo 1) se vincula con la 2-transitividad del grupo S_4. Ella también es equivalente a la representación que corresponde a todas transformaciones de simetría del tetraedro Δ_4 (rotación + reflejo; precisamente estas transformaciones son importantes para la descripción de las oscilaciones de la molécula de fósforo (problema 2, § 2, cap. 1)).

EJEMPLO 4. *Representaciones irreducibles del grupo de cuaterniones Q_8*. Sobre el grupo Q_8 se ha dicho todo en el ejemplo 2, punto 5, § 3, del cap. 7. Allí también se expuso (pero no se llamó por su nombre) la representación irreducible bidimensional $\Phi^{(5)}$ con carácter χ_5.

	1	1	2	2	2
	e	a^2	a	b	ab
χ_1	1	1	1	1	1
χ_2	1	1	—1	—1	1
χ_3	1	1	—1	1	—1
χ_4	1	1	1	—1	—1
χ_5	2	—2	0	0	0

Cuatro representaciones unidimensionales tienen por núcleo el conmutante $\langle a^2\rangle$ y se determinan de la tabla en el ejemplo del punto 3.

EJERCICIOS

1. Obtener la relación (4), escribiendo en forma explícita la expresión $t_{ij} = (\Gamma_i, \chi_j)_G$ para los coeficientes de la descomposición $\Gamma_i = \sum_j t_{ij}\chi_j$ de la función central básica Γ_i (véase (7), § 4) mediante caracteres irreducibles.

2. Comprobar (y recordar sobre el isomorfismo entre el espacio vectorial V y el espacio de funciones lineales V^*, conjugado a él), que la aplicación τ: $A \rightarrow \hat{\hat{A}}$, definida por la condición

$$a^\tau(\chi) = \chi(a),$$

da el isomorfismo del grupo abeliano A en $\hat{\hat{A}}$. (*Indicación*. De $a^\tau(\chi_1\chi_2) = a^\tau(\chi_1)\, a^\tau(\chi_2)$ se deriva, que a^τ es carácter del grupo $\hat{A}$. Como $(aa')^\tau = a^\tau (a')^\tau$, entonces, τ es homomorfismo de A en $\hat{\hat{A}}$. Luego,

$\operatorname{Ker}\tau = \{a \in A \mid a^\tau(\chi) = \chi(a) = 1,\ \forall\chi \in \hat{A}\} \Rightarrow \operatorname{Ker}\tau = e$, y $|\hat{\hat{A}}| = |\hat{A}| = |A| \Rightarrow \tau$ es un isomorfismo.)

Este ejercicio, junto con el teorema 4, establece una parte de la llamada *ley de dualidad para los grupos abelianos finitos*. Una ley análoga, pero mucho más profunda, de dualidad para los grupos abelianos topológicos, que lleva a consecuencias importantes, fue establecida en los años 30 por L. Pontriaguin.

3. Demostrar, que si el grupo abeliano finito A permite una representación irreducible compleja exacta, entonces, A es cíclico.

4. Sean, un grupo abeliano finito A y su subgrupo B. Demostrar, que cualquier carácter del grupo B se continúa hasta el carácter del grupo A y el número de tales proposiciones es igual al índice $(A : B)$.

5. Fundamentar la fase que antecede a los paréntesis al final del ejemplo 3 en el punto 4.

6. ¿A qué es igual la media $\frac{1}{|G|}\sum \chi(g)$ de los valores del carácter complejo χ en los elementos del grupo finito G?

7. Reunir de distintos lugares (véanse: ejemplo 2, p. 2, § 4; ejercicio 4, § 4, ejemplo 1), las tablas referidas al grupo A_5 en la tabla de resumen de los caracteres

	1	15	20	12	12
	e	(12)(34)	(123)	(12345)	(12354)
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1-\sqrt{5})$
χ_3	3	-1	0	$\frac{1}{2}(1-\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$
χ_4	4	0	1	-1	-1
χ_5	*	*	*	*	*

Dar la descripción de los representantes irreducibles con caracteres χ_1, χ_2, χ_3, χ_4. Completar la última fila de la tabla, utilizando la segunda relación de ortogonalidad (4) para los caracteres. (*Respuesta*: 5, 1, -1, 0, 0.)

8. Sean, $P = \{A^iB^jC^k;\ 0 \leqslant i, j, k \leqslant p-1\}$ el grupo de orden p^3 examinado en el ejercicio 3, § 2, cap. 7; $V = \langle e_0, e_1, \ldots, e_{p-1}\rangle_{\mathbb{C}}$ un espacio vectorial complejo de dimensión p; ε, una raíz primitiva de grado p, de 1; $\mathcal{A}$, $\mathcal{B}_h$, $\mathcal{C}_k$, operadores lineales en V, definidos por las relaciones

$$\mathcal{A}e_l = e_{l+1},\quad \mathcal{B}_h e_l = \varepsilon^{-kl}e_l,\quad \mathcal{C}_h e_l = \varepsilon^{k}e_l,\quad 0 \leqslant l \leqslant p-1$$

(los índices inferiores de los elementos básicos se toman de acuerdo con el módulo p).

Mostrar, que la aplicación

$$\Phi^{(k)}: A \longmapsto \mathcal{A},\quad B \longmapsto \mathcal{B}_k,\quad C \longmapsto \mathcal{C}_k$$

da una representación lineal irreducible del grupo P. Las representaciones $\Phi^{(1)}, \ldots, \Phi^{(p-1)}$ no son equivalentes de dos en dos, y, junto con p^2 representaciones unidimensionales (p^2 es el índice del conmutante $P' = \langle C\rangle$ en P), agotan todas las representaciones complejas irreducibles del grupo P.

9. Completar con cálculos los razonamientos siguientes. Sea $D_n = \langle a, b \mid a^n = e,\ b^2 = e,\ bab^{-1} = a^{-1}\rangle$ el grupo de un diedro de orden $2n$, cuyas propiedades (incluyendo la descripción de las clases de elementos conjugados) fueron dadas en el ejemplo 1, p. 5, § 3, cap. 7. Como $\langle a\rangle \lhd D_n$, entonces, las aplicaciones $a \mapsto 1$, $b \mapsto 1$ y $a \mapsto 1$, $b \mapsto -1$ expresan dos representaciones unidimensionales.

Sea $\varepsilon = e^{\frac{2\pi i}{n}}$ la raíz primitiva de n-ésimo grado de 1. Entonces, la aplicación

$$\Phi^{(j)}: a \longmapsto \begin{Vmatrix} \varepsilon^j & 0 \\ 0 & \varepsilon^{-j} \end{Vmatrix},\quad b \longmapsto \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}$$

definirá una representación de grado 2. La representación $\Phi^{(j)}$ irreducible para $j = 1, 2, \ldots, \left[\frac{n-1}{2}\right]$ ($[\alpha]$) es la parte entera del número real α). Para

$n = 2m$ la representación $\Phi^{(m)}$ se descompone en la suma directa de dos representaciones unidimensionales: $a \mapsto -1$, $b \mapsto 1$ y $a \mapsto -1$, $b \mapsto -1$. Esto concuerda con el hecho, que el conmutante D'_{2m} tiene índice 4 en D_{2m} y $D_{2m}/D'_{2m} \cong$ $\cong Z_2 \times Z_2$. Todas las representaciones indicadas son irreducibles y componen un conjunto completo de representaciones complejas irreducibles del grupo del diedro. Hallar la expresión real de la representación $\overline{\Phi}^{(j)}$. Indicar en forma explícita el isomorfismo (equivalencia) $\Phi^{(j)} \approx \Phi^{(k)}$, $k > m$, $j \leqslant m$.

10. *Grupos cristalográficos* (para el problema 2, § 2, cap. 1). Sea, E un espacio euclídeo n-dimensional, y V un espacio vectorial, asociado a E, con producto escalar euclídeo. A cada movimiento d de E le corresponde una transformación lineal ortogonal $\bar{d} \subset O(n)$, además de tal modo, que $\overline{d_1 d_2} = \bar{d}_1 \bar{d}_2$. El grupo D de movimientos del espacio se llama cristalográfico, si la D-órbita de un punto arbitrario es discreta (no tiene puntos límites) y existe un conjunto compacto $M \subset E$, para el que $D(M) = \bigcup\limits_{d \in D} d(M) = E$. Es correcto el teorema de Schoenflies-Biberbach, conforme al cual, el grupo cristalográfico D contiene n traslados afines independientes, que engendran en D el subgrupo normal L, y $\overline{D} \cong D/L$ es un grupo finito (grupo cristalográfico puntual). En total, para $n = 3$, se tienen 32 grupos cristalográficos puntuales geométricamente distintos. Entre ellos, evidentemente, habrá grupos que contengan reflejos (movimientos impropios). De las condiciones de cristalografía se deduce, que toda rotación propia de $\overline{D}$ se expresa por medio de una matriz, semejante a

$$A = \begin{Vmatrix} \cos\theta & -\operatorname{sen}\theta & 0 \\ \operatorname{sen}\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{Vmatrix}$$

con $\operatorname{tr} A = 1 + 2\cos\theta \in \mathbb{Z}$. Apoyándose en el teorema 2, § 3, y en el razonamiento indicado, mostrar, que para $n = 3$ los grupos cristalográficos puntuales sin reflejos serán sólo cíclicos C_1, C_2, C_3, C_4, C_6, diedrales D_2, D_3, D_4, D_6, el grupo del tetraedro **T** y el grupo del cubo (octaedro) **O**.

§ 6. REPRESENTACIONES DE LOS GRUPOS SU(2) Y SO(3)

Las formas concretas, vinculadas con representaciones del grupo SO (3), son parte del pensamiento «físico». La operación SO (3), que pone de manifiesto la simetría de muchos problemas físicos, es interesante desde el punto de vista matemático debido a que, en particular, induce la operación en el espacio de resoluciones de la ecuación $\Delta f = 0$, donde $\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$ es el operador diferencial de Laplace. El análogo bidimensional de este problema fue examinado en el comienzo del capítulo (ejercicio 1).

Todo elemento del grupo SO (3) es producto de varios operadores B_φ, C_θ del tipo (1), § 1, cap. 7. Pero B_φ no opera en z, ni C_θ en x. Por eso, la invariancia de la ecuación $\Delta f = 0$ respecto a B_φ y C_θ se deduce de los cálculos efectuados en el caso bidimensional. Llegamos a la conclusión, que la ecuación $\Delta f = 0$ es invariante con relación a todo el grupo SO (3) o, lo que es lo mismo

$$\Delta f = 0 \Rightarrow \Delta(\Phi_g f) = 0, \quad \forall g \in \mathrm{SO}(3),$$

donde $\Phi_g f$ es una función, definida por la relación

$$(\Phi_g f)(x, y, z) = f(g^{-1}(x), g^{-1}(y), g^{-1}(z)) \quad (1).$$

Por condición, para la transformación ortogonal g^{-1} con matriz $(a_{ij})_1^3$, la columna de nuevas variables tiene la forma

$$\begin{Vmatrix} g^{-1}(x) \\ g^{-1}(y) \\ g^{-1}(z) \end{Vmatrix} = \begin{Vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{Vmatrix} \begin{Vmatrix} x \\ y \\ z \end{Vmatrix}.$$

De acuerdo a (1),

$$\begin{aligned}(\Phi_g(\Phi_h f))(x, y, z) &= (\Phi_h f)(g^{-1}(x), g^{-1}(y), g^{-1}(z)) = \\ &= f(h^{-1}(g^{-1}(x)), h^{-1}(g^{-1}(y)), h^{-1}(g^{-1}(z))) = \\ &= f((gh)^{-1}(x), (gh)^{-1}(y), (gh)^{-1}(z)) = (\Phi_{gh} f)(x, y, z).\end{aligned}$$

Por lo tanto,

$$\Phi_g \Phi_h = \Phi_{gh},$$

o sea, los operadores lineales Φ_g, $g \in SO(3)$, actúan en las funciones de tal modo, que la aplicación $\Phi: g \longmapsto \Phi_g$ resulta representación del grupo SO (3). Este modo muy natural de construcción de representaciones (de hecho, utilizado por nosotros antes, cuando se examinaron las funciones simétricas con grupo de operaciones S_n), en principio sirve para una extensa clase de grupos, y es uno de los métodos típicos de análisis funcional. Es sólo necesario, partiendo de condiciones concretas, elegir el espacio correspondiente de las funciones, y luego dividirlo en subespacios invariantes irreducibles (problema de análisis armónico).

En el caso del grupo SO (3), cuando todas las representaciones irreducibles son finitodimensionales (hecho general para los grupos compactos), como función se toman los polinomios homogéneos

$$f(x, y, z) = \sum_{s, t} a_{s,t} x^s y^t z^{m-s-t}$$

de grado fijo m ($m = 1, 2, 3, \ldots$). Ellos generan el espacio P_m de dimensión $\binom{m+2}{2}$ (véase el ejercicio 4, § 2, cap. 5). Como $\Delta f \in P_{m-2}$, entonces, la condición $\Delta f = 0$ es equivalente a $\binom{m}{2}$ condiciones lineales en coeficientes $a_{s,t}$. Las resoluciones $f \in P_m$ de la ecuación $\Delta f = 0$ se llaman *polinomios armónicos* homogéneos de grado m. En virtud de la linealidad del operador Δ, ellos forman un subespacio H_m de dimensión $\binom{m+2}{2} - \binom{m}{2} = 2m + 1$ (para nosotros $\leqslant 2m + 1$, pero, en realidad, tiene lugar la igualdad). Conforme a lo dicho, H_m es invariante respecto a la operación $\Phi =$

$= \Phi^{(m)}$ del grupo SO (3). Resulta, que es cierto el teorema que dice, que el *espacio* H_m *de la representación* $\Phi^{(m)}$ *es irreducible sobre* **C**, *y cualquier representación del grupo* SO (3) *irreducible sobre* **C** *es equivalente a una de las representaciones* $(\Phi^{(m)}, H_m)$ *de dimensión impar* $2m+1$. En lugar de demostrar este teorema, limitándonos a lo dicho, nos dirigimos al grupo SU (2), donde es un poco más fácil obtener una familia de representaciones irreducibles. En virtud de que se tiene el epimorfismo natural SU (2) $\to$ SO (3) con núcleo de matrices $\pm E$ (véase § 1, cap. 7), toda representación Ψ del grupo SO (3) también se puede considerar representación de SU (2) (véase la demostración del teorema 5, § 5), que cumple la llamada *condición de paridad*: $\Psi_{-E} = \Psi_E$. Además, se sobreentiende, también se cumplirá la igualdad $\Psi_{-g} = \Psi_g$ para todo $g \in$ SU (2). Recíprocamente, cuando la representación Ψ del grupo SU (2) cumple la condición de paridad, al mismo tiempo resulta representación del grupo SO (3). También tienen sentido físico las representaciones de SO (3) de «doble signo», o sea, las representaciones del grupo SU (2) que no cumplen la condición de paridad. A éstas se refiere, por ejemplo, la representación bidimensional común (de spin).

Señalemos además, que cualquier representación irreducible del grupo SO (3), distinta de la unidad, resulta exacta, tal como se deduce de carácter simple de SO (3) (teorema 6, § 3, cap. 7).

TEOREMA 1. *Sea* $V_n = \langle x^k y^{n-k} \mid k = 0, 1, \ldots, n\rangle_{\mathbf{C}}$ *el espacio de los polinomios homogéneos de grado* n, *de dos variables complejas, con operación* $\Psi^{(n)}$ *del grupo* SU (2) *en él, definida por la regla*

$$(\Psi_g^{(n)} f)(x, y) = f(\bar{\alpha}x - \beta y, \bar{\beta}x + \alpha y)$$

para cada elemento

$$g = \begin{Vmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{Vmatrix}, \quad |\alpha|^2 + |\beta|^2 = 1.$$

Entonces, $(\Psi^{(n)}, V_n)$ *es una representación irreducible de* SU (2) *de dimensión* $n+1$. *Para* n *par*, $(\Psi^{(n)}, V_n)$ *también es una representación irreducible del grupo* SO (3).

DEMOSTRACION. Supongamos, que el polinomio

$$f(x, y) = \sum_{k=0}^{n} a_k x^k y^{n-k} \neq 0$$

está contenido en algún subespacio invariante $U \subset V_n$. Entonces, también

$$\sum_{k=0}^{n} (e^{-i\varphi})^k a_k x^k y^{n-k} = e^{-in\frac{\varphi}{2}} (\Psi_{b_\varphi}^{(n)} f)(x, y) \in U,$$

donde b_φ es un elemento de SU (2) del tipo (4), § 1, cap. 7. Como φ es un número real arbitrario del intervalo $(0, 2\pi)$, se puede componer

un sistema lineal con determinante de Vandermonde, del cual se sigue, que

$$f(x, y) \in U \Rightarrow x^k y^{n-k} \in U \qquad (2)$$

para cualquier monomio con coeficiente $a_k \neq 0$. Pero, si $x^k y^{n-k} \in U$ para algún k, entonces

$$\bar{\alpha}^k \bar{\beta}^{n-k} x^m + a \ldots = (\bar{\alpha}x - \beta y)^k (\bar{\beta}x + \alpha y)^{n-k} = \Psi_g^{(n)}(x^k y^{n-k}) \in U,$$

Tomando g con $\alpha\beta \neq 0$, llegamos, en virtud de (2), a la conclusión de que $x^n \in U$, lo que a su vez nos da

$$\sum_{s=0}^{n} \binom{n}{s} \bar{\alpha}^s (-\beta)^{n-s} x^s y^{n-s} \in U.$$

Como $\binom{n}{s} \bar{\alpha}^s (-\beta)^{n-s} \neq 0$, entonces, $x^s y^{n-s} \in U$, $s = 0, 1, \ldots, n$. Por lo tanto, $U = V_n$, y la irreducibilidad de $(\Psi^{(n)}, V_n)$ queda demostrada.

Luego

$$\Psi_{-E}^{(n)}(x^k y^{n-k}) = (-x)^k (-y)^{n-k} = (-1)^n x^k y^{n-k},$$

así, que para $n = 2m$ se cumple la condición de paridad (véase la observación más arriba) y $(\Psi^{(2m)}, V_{2m})$ puede considerarse representación irreducible de dimensión $2n + 1$. ∎

De hecho, $\Psi^{(2m)}$ es equivalente a la representación $\Phi^{(m)}$ del grupo SO (3) en el espacio de los polinomios armónicos homogéneos de grado m, pero no nos detenemos en esto, así como no intentamos (aunque es posible) elegir en V_n una base tal, que la representación $\Psi^{(n)}$ se vuelva unitaria. Observemos solamente, empleando la terminología del análisis tensorial, que la representación $\Psi^{(n)}$ del grupo SU (2) también se realiza en clase de tensores simétricos covariantes de rango n. La teoría completa, y suficientemente transparente, de las representaciones de grupos compactos, incluyendo SU(2) y SO(3), habitualmente se desarrolla en los límites del método infinitesimal, apoyándose en la correspondencia entre los grupos y el álgebra de Lie.

EJERCICIOS

1. Formular $2m + 1$ polinomios armónicos homogéneos y linealmente independientes de grado m.

2. Mostrar que todo polinomio homogéneo $f \in P_m$ se escribe en forma de combinación lineal con coeficientes que dependen de $x^2 + y^2 + z^2$, polinomios armónicos de grados m, $m - 2$, $m - 4$, ... (*Indicación*. Igualando las dimensiones, obtener una descomposición en la suma directa de espacios

$$P_m = H_m \oplus (x^2 + y^2 + z^2) H_{m-2} \oplus (x^2 + y^2 + z^2)^2 \times H_{m-4} \oplus \ldots)$$

3. Deducir del ejercicio 2, que toda función polinómica $\tilde{g}$: $(X, Y, Z) \mapsto g(x, y, z)$ en la esfera S^2: $x^2 + y^2 + z^2 = 1$ se descompone en *funciones esféricas*, o sea, en limitaciones de polinomios armónicos en S^2.

4. Mostrar, sin recurrir a una descripción completa de las representaciones irreducibles del grupo SO (3), que el homomorfismo τ: SO (3) $\to$ SU (2) puede ser sólo trivial. (*Indicación*. En virtud de que SO (3) es simple, la no trivialidad de τ significaría que τ es una representación exacta de grado 2. Pero, como se ve del ejemplo 3, p. 4, § 5, o de la descripción de los subgrupos finitos en SU (2) (véase § 3), incluso la limitación $\tau\,|_{S_4 \cong O}$ no puede ser exacta.)

§ 7. PRODUCTO TENSORIAL DE REPRESENTACIONES

1. Representación contragradiente. Sea (Φ, V) una representación del grupo G sobre el campo $\mathbb{C}$. Pongamos a consideración el espacio dual V^* (de funciones lineales en V) hagamos

$$(\Phi^* (g)\cdot f)(v) = f(\Phi(g^{-1})v); \quad f \in V^*, \ v \in V. \tag{1}$$

La linealidad del operador $\Phi^*(g)$ se comprueba de inmediato. Elijamos, luego, en V y V^* las bases duales

$$V = \langle e_1, \ldots, e_n \rangle, \quad V^* = \langle f_1, \ldots, f_n \rangle, \quad f_i(e_j) = \delta_{ij}.$$

La matriz del operador lineal $\Phi^*(g)$ en la base $f_1, \ldots, f_n$, es traspuesta a la matriz del operador $\Phi(g^{-1})$ en la base $e_1, \ldots, e_n$:

$$\Phi^*_g = {}^t\Phi_{g^{-1}}. \tag{2}$$

Como

$$\Phi^*_{gh} = {}^t\Phi_{(gh)^{-1}} = {}^t\Phi_{h^{-1}g^{-1}} = {}^t(\Phi_{h^{-1}}\Phi_{g^{-1}}) = {}^t\Phi_{g^{-1}}{}^t\Phi_{h^{-1}} = \Phi^*_g\Phi^*_h,$$

entonces, la relación (2) (o (1)) se determina, hablando en general, por la nueva representación lineal (Φ^*, V^*), del grupo G, denominada representación *contragradiente* (o *dual*) respecto a (Φ, V). La necesidad de examinar tales representaciones, surge cada vez, cuando a un grupo que opera en vectores (tensores contravariantes), los hacemos operar en coordenadas de vectores (tensores covariantes), como, de hecho, sucedió en el § 6. Como se puede apreciar fácilmente, por ejemplo de (2), $(\Phi^*)^* \approx \Phi$. Las representaciones recíprocamente contragradientes, pueden no distinguirse o ser equivalentes. Si, digamos, (Φ, G) es una representación ortogonal real, entonces, $\Phi^*_g = {}^t\Phi_g^{1} = \Phi_g$. Pero, en el caso general, las representaciones Φ^* y Φ no son equivalentes, como lo muestra este ejemplo sencillo:

$$C_3 = \langle a \mid a^3 = e \rangle; \quad \Phi(a) = \varepsilon\ ,$$
$$\Phi^*(a) = \varepsilon^{-1}\ (\varepsilon^2 + \varepsilon + 1 = 0).$$

Para el grupo finito G, el criterio exacto de equivalencia de las representaciones contragradientes se obtiene en el lenguaje de la teoría de caracteres. Puesto que los polinomios característicos de las matrices A y ${}^tA$ coinciden:

$$\det(\lambda E - {}^tA) = \det {}^t(\lambda E - A) = \det(\lambda E - A),$$

de las propiedades elementales de los caracteres (proposición § 4), se deduce, que

$$\chi_{\Phi^*}(g) = \overline{\chi_{\Phi}(g)}.$$

En particular, la representación Φ con carácter que adopta sólo valores reales, es equivalente a Φ^*. Por supuesto, siempre

$$(\chi_{\Phi^*}, \chi_{\Phi^*})_G = (\chi_{\Phi}, \chi_{\Phi})_G,$$

así que Φ^*, Φ son a un mismo tiempo reducibles o irreducibles.

2. Producto tensorial de representaciones. En el curso de álgebra lineal y geometría (véase también el ejercicio 1), se demuestra la afirmación siguiente:

TEOREMA 1. *Sean V, W, espacios vectoriales sobre el campo P. Entonces, existe el espacio vectorial T sobre P y la aplicación bilineal τ: $V \times W \to T$, que cumple las condiciones:*

(T1) *si $v_1, \ldots, v_k \in V$ son linealmente independientes y $w_1, \ldots$ $\ldots, w_k \in W$, se tendrá $\sum_{i=1}^{k} \tau(v_i, w_i) = 0 \Rightarrow w_1 = 0, \ldots, w_k = 0$;*

(T2) *si $w_1, \ldots, w_k \in W$ son linealmente independientes, entonces, $\sum_i \tau(v_i, w_i) = 0 \Rightarrow v_1 = 0, \ldots, v_k = 0$;*

(T3) *τ es una aplicación sobreyectiva, o sea*

$$T = \langle \tau(v, w) \mid v \in V,\ w \in W \rangle_P.$$

Además, el par (τ, T) es universal, en el sentido que, cualquiera que sea el par (τ', T'), compuesto por el espacio vectorial T' y la aplicación bilineal τ': $V \times W \to T'$, existe una aplicación lineal única σ: $T \to T'$, para la cual $\tau'(v, w) = \sigma(\tau(v, w))$, $v \in V$, $w \in W$. ∎

Suponiendo la existencia de dos pares universales (τ, T), (τ', T'), descubrimos fácilmente, que las aplicaciones lineales σ: $T \to T'$, σ': $T' \to T$, resultan de hecho isomorfismos recíprocamente inversos: $\sigma' \circ \sigma = e_T$, $\sigma \circ \sigma' = e_{T'}$. De este modo, $T \cong T'$, además, el isomorfismo σ: $T \to T'$ posee la propiedad indicada en la formulación del teorema.

Si el par (τ, T) está determinado unívocamente, con exactitud hasta el isomorfismo, mediante los espacios vectoriales dados V, W, entonces se denomina *producto tensorial* de estos espacios. Escribiendo $T = V \otimes_P W$, o, sencillamente, $T = V \otimes W$, debemos aun recordar, que el espacio vectorial T está provisto de la aplicación bilineal $(v, w) \mapsto v \otimes w$ del producto cartesiano $V \otimes W$ en T, que cumplen las condiciones (T1), (T2) y (T3). Así pues, como elementos del producto tensorial $V \otimes W$ sirven las combinaciones lineales formales con coeficientes de P pares ordenados $v \otimes w$, con $v \in V$, $w \in W$.

Asimismo, se presuponen cumplidas las condiciones siguientes:

$$(v_1 + v_2) \otimes w - v_1 \otimes w - v_2 \otimes w = 0, \qquad (3)$$
$$v \otimes (w_1 + w_2) - v \otimes w_1 - v \otimes w_2 = 0,$$
$$\lambda v \otimes w - v \otimes \lambda w = 0, \ \lambda \in P$$
$$(\lambda (v \otimes w) = \lambda v \otimes w = v \otimes \lambda w).$$

En el teorema 1, se aprecia inmediatamente, que las aplicaciones biyectivas $v \otimes w \mapsto w \otimes v$, $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$, $v \otimes \lambda \mapsto$ $\mapsto \lambda \otimes v \mapsto \lambda v$ establecen los isomorfismos, llamados *canónicos*, de los espacios vectoriales:

$$V \otimes W \cong W \otimes V,$$
$$(U \otimes V) \otimes W \cong U \otimes (V \otimes W),$$
$$V \otimes P \cong P \otimes V \cong V.$$

También se cumplen las leyes de distribución:

$$(U \oplus V) \otimes W \cong (U \otimes W) \oplus (V \otimes W),$$
$$U \otimes (V \oplus W) \cong (U \otimes V) \oplus (U \otimes W).$$

En el análisis tensorial, de donde son originarios los conceptos aquí examinados, se estudian productos tensoriales de tipo especial:

$$\underbrace{V^* \otimes \ldots \otimes V^*}_{p} \otimes \underbrace{V \otimes \ldots \otimes V}_{q}.$$

Sus elementos son tensores del tipo (p, q), p veces covariantes y q veces contravariantes. Al elegir las bases duales $e_1, \ldots, e_n$ en V y $e^1, \ldots, e^n$ en V^*, los elementos $e^{i_1} \otimes \ldots \otimes e^{i_p} \otimes e_{j_1} \otimes \ldots$ $\ldots \otimes e_{j_q}$ componen la base del espacio de tensores del tipo (p, q). Habitualmente, se entiende por tensor simplemente el cúmulo de coordenadas $\left\{ t_{i_1 \ldots i_p}^{j_1 \ldots j_q} \right\}$ en esta base, con indicación de la regla de cambio de coordenadas al pasar de un sistema básico a otro. Precisamente así se obtiene la interpretación en el lenguaje tensorial (de hecho, en el matricial) de tales conceptos como forma bilineal y operador lineal. Limitándose a estas breves referencias, que no pensamos utilizar de un modo pleno, nos dirigimos a la cuestión que nos interesa sobre las representaciones.

Sean $\mathcal{A}: V \to V$, $\mathcal{B}: W \to W$ operadores lineales. Se llama *producto tensorial* de los mismos el operador lineal

$$\mathcal{A} \otimes \mathcal{B}: V \otimes W \to V \otimes W,$$

que opera de acuerdo con la regla

$$(\mathscr{A} \otimes \mathscr{B})(v \otimes w) = \mathscr{A}v \otimes \mathscr{B}w \tag{4}$$

(luego, por linealidad: $(\mathscr{A} \otimes \mathscr{B})(\sum v_i \otimes w_i) = \sum \mathscr{A}v_i \otimes \mathscr{B}w_i$). Es claro, que esta definición concuerda con las relaciones (3). Por ejemplo,

$$\mathscr{A}(v_1+v_2) \otimes \mathscr{B}w - \mathscr{A}v_1 \otimes \mathscr{B}w - \mathscr{A}v_2 \otimes \mathscr{B}w =$$
$$= (\mathscr{A}v_1 + \mathscr{A}v_2) \otimes \mathscr{B}w - \mathscr{A}v_1 \otimes \mathscr{B}w - \mathscr{A}v_2 \otimes \mathscr{B}w = 0.$$

Por eso, la operación $\mathscr{A} \otimes \mathscr{B}$ en $V \otimes W$ está dada correctamente. Hagamos notar también, las relaciones siguientes, que se deducen inmediatamente de la definición (4):

$$(\mathscr{A} \otimes \mathscr{B})(\mathscr{C} \otimes \mathscr{D}) = \mathscr{A}\mathscr{C} \otimes \mathscr{B}\mathscr{D},$$
$$(\mathscr{A} + \mathscr{C}) \otimes \mathscr{B} = \mathscr{A} \otimes \mathscr{B} + \mathscr{C} \otimes \mathscr{B},$$
$$\mathscr{A} \otimes (\mathscr{B} + \mathscr{D}) = \mathscr{A} \otimes \mathscr{B} + \mathscr{A} \otimes \mathscr{D},$$
$$\mathscr{A} \otimes \lambda\mathscr{B} = \lambda\mathscr{A} \otimes \mathscr{B} = \lambda(\mathscr{A} \otimes \mathscr{B}).$$

La comprobación se la dejamos al lector.

Sean, como antes, $V = \langle e_1, \ldots, e_n \rangle$, $W = \langle f_1, \ldots, f_m \rangle$. Obtenemos la matriz $A \otimes B$ de dimensión $nm \times nm$ del operador $\mathscr{A} \otimes \mathscr{B}$ en la base

$$\{e_1 \otimes f_1, \ldots, e_1 \otimes f_m, e_2 \otimes f_1, \ldots, e_2 \otimes f_m, \ldots, e_n \otimes f_1, \ldots, \ldots, e_n \otimes f_m\},$$

observando, que

$$\mathscr{A}e_i = \sum_{i'} \alpha_{i'i} e_{i'}, \quad \mathscr{B}f_j = \sum_{j'} \beta_{j'j} f_{j'},$$
$$(\mathscr{A} \otimes \mathscr{B})(e_i \otimes f_j) = \sum_{i', j'} \alpha_{i'i}\beta_{j'j} e_{i'} \otimes f_{j'}.$$

Por lo tanto, con $A = (\alpha_{i'i})$, $B = (\beta_{j'j})$ tenemos

$$A \otimes B = (\alpha_{i'i}\beta_{j'j}) = \left\| \begin{matrix} \alpha_{11}B & \alpha_{12}B & \ldots & \alpha_{1n}B \\ \alpha_{21}B & \alpha_{22}B & \ldots & \alpha_{2n}B \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{n1}B & \alpha_{n2}B & \ldots & \alpha_{nn}B \end{matrix} \right\|.$$

En particular, tenemos la fórmula para la traza

$$\operatorname{tr} A \otimes B = \alpha_{11} \operatorname{tr} B + \alpha_{22} \operatorname{tr} B + \ldots + \alpha_{nn} \operatorname{tr} B = \operatorname{tr} A \cdot \operatorname{tr} B. \tag{5}$$

De paso, observemos, que

$$\det A \otimes B = \det (A \otimes E_m)(E_n \otimes B) =$$
$$= \det A \otimes E_m \cdot \det E_n \otimes B = (\det A)^m (\det B)^n,$$

así que la degeneración de los operadores $\mathscr{A}$ y $\mathscr{B}$ conlleva la degeneración de su producto tensorial $\mathscr{A} \otimes \mathscr{B}$.

Sean ahora (Φ, V), (Ψ, W) dos representaciones lineales del grupo G con caracteres χ_Φ y χ_Ψ, respectivamente. Determinemos de un modo común la representación $(\Phi \otimes \Psi, V \otimes W)$, haciendo

$$(\Phi \otimes \Psi)(g) = \Phi(g) \otimes \Psi(g), \quad \forall g \in G.$$

De las propiedades generales del producto tensorial de operadores lineales y de la fórmula (5) se deriva que la aplicación $\Phi \otimes \Psi$ brindará realmente una representación del grupo G con espacio de representación $V \otimes W$ y con carácter

$$\chi_{\Phi \otimes \Psi} = \chi_\Phi \chi_\Psi. \tag{6}$$

Diremos, que $(\Phi \otimes \Psi, V \otimes W)$ es *producto tensorial de las representaciones* (Φ, V) y (Ψ, W). Para $\Psi = \Phi$, $W = V$ se habla también sobre el *cuadrado tensorial*. En el segundo miembro de la fórmula (6) hay un producto corriente común de las funciones centrales χ_Φ y χ_Ψ.

Es totalmente evidente, que si U es subespacio G-invariante en V, entonces, también $U \otimes W$ será subespacio G-invariante en $V \otimes W$. Una observación análoga puede hacerse respecto al subespacio G-invariante en W. Pero, de la irreducibilidad de V y W, en general no se deduce que $V \otimes W$ es irreducible, tal como lo muestra el ejemplo del cuadrado tensorial $\Phi^{(3)} \otimes \Phi^{(3)}$ de la representación bidimensional del grupo S_3 (véase la tabla en el punto 2, § 5). El efecto, $\dim_{\mathbb{C}} \Phi^{(3)} \otimes \Phi^{(3)} = 4$, y el grado máximo de la representación irreducible del grupo S_3, es igual a 2.

La cuestión de la descripción efectiva de las representaciones irreducibles, contenidas en $\Phi \otimes \Psi$ y, más generalmente, en el producto tensorial $\Phi^{(1)} \otimes \Phi^{(2)} \otimes \ldots \otimes \Phi^{(p)}$ de varias representaciones lineales, tiene un significado fundamental, porque muchas representaciones de grupos importantes y muy naturales, surgen como productos tensoriales. Precisamente, desde este punto de vista hay que mirar a las representaciones de los grupos SU (2) y SU (3) (véase el § 6), y también a los ejemplos 3 y 4 del punto 2, § 1. Los subespacios invariantes de tensores covariantes (o contravariantes) simétricos y antisimétricos, permanentemente se encuentran en distintas aplicaciones geométricas. El problema considerado es atractivo especialmente cuando es cierto el teorema sobre la reducibilidad total de las representaciones.

3. Anillo de caracteres. Por simpleza, nos limitamos al caso del grupo finito G y campo $\mathbb{C}$. Sean, $\Phi^{(1)}, \Phi^{(2)}, \ldots, \Phi^{(r)}$, el conjunto completo de representaciones irreducibles no equivalentes de dos en dos del grupo G sobre $\mathbb{C}$, y $\chi_1, \chi_2, \ldots, \chi_r$ sus caracteres correspondientes (r es el número de clases de elementos conjugados en G). Sabemos que

$$\Phi \otimes \Psi \approx m_1\Phi^{1} + \ldots + m_r\Phi^{(r)},$$

donde las multiplicidades m_i dependen únicamente de Φ y Ψ. Según la fórmula (6)

$$\chi_\Phi \chi_\Psi = m_1\chi_1 + \ldots + m_r\chi_r.$$

Sea $X_{\mathbb{Z}}(G)$ el conjunto de todas las combinaciones lineales enteras posibles de los caracteres $\chi_1, \ldots, \chi_r$. Ya hemos demostrado, que $\chi_1, \ldots, \chi_r$ es la base ortonormal del espacio $X_{\mathbb{C}}(G)$, por eso, $X_{\mathbb{Z}}(G) \subset X_{\mathbb{C}}(G)$ es, en todo caso, un grupo abeliano libre $\cong \mathbb{Z}^r$ con generadores $\chi_1, \ldots, \chi_r$. Sus elementos se llaman *caracteres generalizados* del grupo G. Caracteres verdaderos resultarán sólo las combinaciones $\sum m_i\chi_i$ con $m_i \geqslant 0$.

De lo precedente se aprecia, que el producto tensorial de representaciones, induce en $X_{\mathbb{Z}}(G)$ una operación algebraica binaria, o sea, conmutativa, asociativa, sometida a las leyes de distributividad. Hablando con brevedad, es correcto el

TEOREMA 2. *Los caracteres generalizados generan el anillo conmutativo asociativo* $X_{\mathbb{Z}}(G)$ *con unidad que es el carácter unitario* χ_1.

$X_{\mathbb{C}}(G)$ se llama álgebra conmutativa asociativa de dimensión r sobre $\mathbb{C}$. La estructura del anillo $X_{\mathbb{Z}}(G)$ (del álgebra $X_{\mathbb{C}}(G)$), queda completamente determinada por *las constantes estructurales*, o sea, por los números enteros m_{ij}^k de las relaciones

$$\chi_i\chi_j = \sum m_{ij}^k\chi_k. \tag{7}$$

En particular, las igualdades $m_{ij}^k = m_{ji}^k$, $m_{1j}^k = \delta_{kj}^k$ reflejan las propiedades de conmutatividad de $X_{\mathbb{Z}}(G)$ y de unicidad de χ_1. De acuerdo con (7)

$$\chi_i(g)\chi_j(g) = \sum m_{ij}^k\chi_k(g), \quad \forall g \in G.$$

Multiplicando ambos miembros de esta relación por $\frac{1}{|G|}\overline{\chi_s(g)}$, sumando con respecto a $g \in G$ y utilizando la primera relación de ortogonalidad para los caracteres, obtendremos

$$m_{ij}^s = \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_j(g)\overline{\chi_s(g)}. \quad \blacksquare \tag{8}$$

De este modo, las constantes estructurales se expresan en términos de los propios caracteres.

De (8) se puede extraer una afirmación simple. Precisamente,

$$m_{ij}^1 = \frac{1}{|G|}\sum_g \chi_i(g)\chi_j(g)\overline{\chi_1(g)} = \frac{1}{|G|}\sum_g \chi_i(g)\chi_j(g) =$$
$$= \frac{1}{|G|}\sum_g \chi_i(g)\overline{\overline{\chi_j(g)}} = (\chi_i, \chi_j^*)_G,$$

donde $\chi_j^* = \chi_{\Phi^{(j)}*}$ es carácter de una representación contragradiente a $\Phi^{(j)}$ (véase el punto 1). Por lo tanto, *la representación unidad entra en calidad de componente en la descomposición* $\Phi^{(i)} \otimes \Phi^{(j)}$ *si, y sólo si,* $\Phi^{(i)}$ *es equivalente a la representación* $\Phi^{(j')} = \Phi^{(j)} *$ (en caso contrario, $m_{ij}^1 = (\chi_i, \chi_j^*)_G = 0$). ∎

Notemos también, que el *producto tensorial de una representación unidimensional* $\Phi^{(i)}$ *por una representación irreducible arbitraria* $\Phi^{(j)}$, *resulta siempre una representación irreducible de la misma dimensión que* $\Phi^{(j)}$. Esto es bastante comprensible sin ninguna explicación y formalmente se deduce del criterio de irreducibilidad de los caracteres. Si $\chi = \chi_{\Phi^{(i)}\otimes\Phi^{(j)}} = \chi_i\chi_j$, entonces, $\chi_i(g)$ resulta raíz compleja de alguna potencia de 1 y $\chi_i(g)\overline{\chi_i(g)} = 1$, siendo, por eso,

$$(\chi, \chi)_G = \frac{1}{|G|}\sum_g \chi_i(g)\chi_j(g)\overline{\chi_i(g)}\,\overline{\chi_j(g)} =$$

$$= \frac{1}{|G|}\sum_g \chi_j(g)\overline{\chi_j(g)} = (\chi_j, \chi_j)_G = 1. \ ∎$$

EJEMPLO 1. $G = S_3$ (véanse las tablas en el p. 1, § 2, y en el p. 2, § 5):

$$\Phi^{(1)} \otimes \Phi^{(3)} \approx \Phi^{(2)} \otimes \Phi^{(3)} \approx \Phi^{(3)}.$$

EJEMPLO 2. $G = S_4$ (véase el ejemplo 3, p. 4, § 5):

$$\Phi^{(2)} \times \Phi^{(1)} \approx \Phi^{(5)},$$

$$\Phi^{(2)} \times \Phi^{(0)} \approx \Phi^{(4)}.$$

Finalmente, demostremos el interesante teorema que sigue, generalizador del teorema 2 del § 5 sobre la descomposición de una representación regular.

TEOREMA 3. *Sea* $\chi = \chi_\Phi$ *el carácter de la representación exacta* (Φ, V) *del grupo finito* G *sobre el campo de los números complejos* $\mathbb{C}$, *que toma en* G *exactamente* m *valores distintos. Entonces, cada carácter irreducible* χ_k *entra con coficiente no nulo en la descomposición de por lo menos un carácter* $\chi^0 = \chi_1, \chi, \chi^2, \ldots, \chi^{m-1}$. *Con otras palabras, toda representación irreducible se halla contenida en la descomposición de alguna potencia tensorial* $\Phi^{\otimes i} = \Phi \otimes \ldots \otimes \Phi$, $0 \leqslant i \leqslant m-1$, de cualquier *representación exacta* Φ.

DEMOSTRACIÓN. Sean $\omega_j = \chi(g_j)$, $j = 0, 1, \ldots, m-1$ valores distintos, tomados por el carácter χ en G, además, $\omega_0 = \chi(e) = \deg \Phi$. Sea, luego,

$$G_j = \{g \in G \mid \chi(g) = \chi(g_j) = \omega_j\}.$$

En virtud de la exactitud de la representación Φ, tenemos

$$G_0 = \operatorname{Ker} \Phi = \{e\}.$$

Sea χ_k un carácter irreducible del grupo G, que no entra en la descomposición de ninguno de los caracteres χ^i. Entonces,

$$0 = |G|\,(\chi^i, \chi_k)_G = \sum_{j=0}^{m-1} (\chi(g_j))^i \sum_{g\in G_j} \overline{\chi_k(g)} = \sum \omega_j^i T_j, \quad 0 \leqslant i \leqslant m-1,$$

es un sistema homogéneo de ecuaciones lineales respecto a $T_j = \sum_{g\in G_j} \overline{\chi_k(g)}$, con determinante

$$\det(\omega_j^i) = \begin{Vmatrix} 1 & 1 & 1 \\ \omega_0 & \omega_1 & \omega_{m-1} \\ \dots & \dots & \dots \\ \omega_0^{m-1} & \omega_1^{m-1} & \omega_{m-1}^{m-1} \end{Vmatrix},$$

diferentes de cero (determinante de Vandermonde). De este modo, $T_j = 0$, $j = 0, 1, \ldots, m-1$, o sea,

$$\sum_{g\in G_j} \chi_k(g^{-1}) = 0, \quad j = 0, 1, \ldots, m-1.$$

En particular,

$$0 = \sum_{g\in G_0} \chi_k(g^{-1}) = \chi_k(e)$$

es una contradicción, que demuestra el teorema.

En caso de la representación regular ρ, evidentemente, $m = 2$.

4. Invariantes de grupos lineales. Llamamos habitualmente grupo lineal de grado n, cualquier subgrupo en GL (n, K), donde K es algún campo. En adelante se puede tomar $K = \mathbb{R}$ o $\mathbb{C}$. Si G es un grupo abstracto y Φ: $G \to$ GL $(n, \mathbb{C})$ su representación lineal, entonces, al par (G, Φ) también lo denominaremos grupo lineal. Las transformaciones lineales Φ_g operan en las columnas de variables $x_1, \ldots, x_n$:

$$\begin{Vmatrix} \Phi_g(x_1) \\ \cdot \\ \cdot \\ \cdot \\ \Phi_g(x_n) \end{Vmatrix} = \Phi_g \begin{Vmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{Vmatrix}.$$

Ellas convierten cualquier forma (polinomio homogéneo) f de grado m, nuevamente en una forma de grado m:

$$(\widetilde{\Phi}_g f)(x_1, \ldots, x_n) = f(\Phi_{g^{-1}}(x_1), \ldots, \Phi_{g^{-1}}(x_n)).$$

Distintos casos particulares de esta operación ya han sido tratados (véase el § 6). La aplicación $\widetilde{\Phi}$ define la representación del grupo G en el espacio P_m de formas sobre $\mathbb{C}$ de grado m (como tensores simétricos covariantes de rango m).

DEFINICION. La forma $f \in P_m$, que queda inmóvil con la operación $\widetilde{\Phi}_g$ ($\widetilde{\Phi}_g f = f$, $\forall g \in G$), se llama *invariante* (*entera*) de grado m del grupo lineal (G, Φ).

En efecto, debería haberse tomado el polinomio de coeficientes de la forma «general» de grado m, que queda en su lugar con la operación $\widetilde{\Phi}(G)$. Así proceden en la teoría general de invariantes, pero nosotros, para simplificar, nos limitamos a la definición dada. Si en calidad de f se toma una función racional, entonces, se puede pasar al concepto de *invariante racional*. Es importante también la idea de *invariante relativo* de f, cuando

$$\widetilde{\Phi}_g f = \omega_g f,$$

donde $\omega_g \in \mathbb{C}$ es un multiplicador, dependiente del elemento $g \in G$.

Es claro, que cualquier conjunto $\{f_1, f_2, \ldots\}$ de invariantes del grupo lineal (G, Φ) engendra en $\mathbb{C}[x_1, \ldots, x_n]$ el subanillo $\mathbb{C}[f_1, f_2, \ldots]$ de invariantes.

Examinemos un pequeño número de ejemplos.

EJEMPLO 1. La forma cuadrática $x_1^2 + x_2^2 + \ldots + x_n^2$ y cualesquiera polinomios de ella, resultan invariantes enteros del grupo ortogonal $O(n)$.

EJEMPLO 2. Los polinomios simétricos elementales $s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)$ son invariantes enteros del grupo simétrico S_n examinado junto con el monomorfismo canónico Φ: $S_n \to GL(n)$. El teorema fundamental sobre polinomios simétricos afirma, que los invariantes $s_1, \ldots, s_n$, de grados 1, 2, ..., n, son algebraicamente independientes, y con las funciones polinómicas (racionales) de los mismos, se agotan todos los invariantes enteros (racionales) del grupo (S_n, Φ).

Los polinomios antisimétricos $\Phi_\pi f = (\det \Phi_\pi) f = \varepsilon_\pi f$, sirven de invariantes relativos del grupo lineal (S_n, Φ). Hemos visto (ejercicio 3, § 2 cap. 6), que cualquier polinomio antisimétrico f tiene la forma $f = \Delta_n \cdot g$, donde $\Delta_n = \prod_{j<i} (x_i - x_j)$, y g es un polinomio simétrico arbitrario, o sea, un invariante absoluto.

EJEMPLO 3. A la representación Φ_A: $X \to AXA^{-1}$ de grado n^2, del grupo lineal completo $GL(n, K)$, con espacio de representación $M_n(K)$ (véase el ejemplo 3 del § 1), le responde un sistema de n invariantes algebraicamente independientes, que son coeficientes del polinomio característico de la matriz $X = (x_{ij})$. A ellos pertenecen, en particular, los invariantes, bien conocidos por nosotros, $\operatorname{tr} X = \sum x_{ii}$ y $\det X$.

EJEMPLO 4. En la forma cuadrática $f(x_1, \ldots, x_n) = \sum a_{ij} x_i x_j$, escrita del modo $f(x_1, \ldots, x_n) = {}^tXAX$, $A = (a_{ij}) = {}^tA$, $X = [x_1, \ldots, x_n]$, opera el grupo ortogonal $O(n)$:

$$C \in O(n) \Rightarrow (C^{-1}f)(x_1, \ldots, x_n) = {}^t(CX)A(CX) = {}^tX\,{}^tCACX = {}^tX(C^{-1}AC)X.$$

En este caso, se habla sobre invariantes de la forma cuadrática f respecto a $O(n)$: $\operatorname{tr} A, \ldots, \det A$. Para la forma cuadrática binaria $ax^2 + 2bxy + cy^2$, los invariantes $a + c$ y $ac - b^2$, que caracterizan métricamente distintas clases de curvas de segundo orden, son conocidos también del curso de geometría analítica.

EJEMPLO 5. Consideremos el grupo simétrico S_3 como lineal de grado 2, utilizando la representación Γ equivalente a la $\Phi^{(3)}$, de la tabla al final del punto 1, § 2:

$$\Gamma_{(123)}=\begin{Vmatrix}\varepsilon & 0\\ 0 & \varepsilon^{-1}\end{Vmatrix},\quad \Gamma_{(23)}=\begin{Vmatrix}0 & 1\\ 1 & 0\end{Vmatrix},\quad \varepsilon^2+\varepsilon+1=0$$

(la equivalencia se efectúa por medio de la conjugación

$$\begin{Vmatrix}\varepsilon & 0\\ 0 & 1\end{Vmatrix}\Phi_\sigma^{(3)}\begin{Vmatrix}\varepsilon^{-1} & 0\\ 0 & 1\end{Vmatrix}=\Gamma_\sigma).$$

Sean u, v variables independientes, transformables linealmente mediante Γ_σ:

$$\Gamma_{(123)}(u)=\varepsilon u,\quad \Gamma_{(123)}(v)=\varepsilon^{-1}v,\quad \Gamma_{(23)}(u)=v,\quad \Gamma_{(23)}(v)=u.$$

Como

$$\widetilde{\Gamma}_{(123)}(uv)=\Gamma^{-1}_{(123)}(u)\,\Gamma^{-1}_{(123)}(v)=\varepsilon^{-1}u\cdot\varepsilon v=uv,$$
$$\widetilde{\Gamma}_{(23)}(uv)=vu=uv,$$
$$\widetilde{\Gamma}_{(123)}(u^3+v^3)=(\varepsilon^{-1}u)^3+(\varepsilon v)^3=u^3+v^3,$$
$$\widetilde{\Gamma}_{(23)}(u^3+v^3)=v^3+u^3=u^3+v^3,$$

entonces, el grupo $(S_3,\ \Gamma)$ tiene la forma

$$I_1=uv,\qquad I_2=u^3+v^3 \tag{9}$$

de grados 2 y 3, en calidad de sus invariantes.

Luego, el grupo S_3 opera de modo natural en los polinomios $f(x_1,\ x_2,\ x_3)$ de tres variables independientes:

$$(\sigma f)(x_1,\ x_2,\ x_3)=f(x_{\sigma^{-1}(1)},\ x_{\sigma^{-1}(2)},\ x_{\sigma^{-1}(3)}).$$

Haciendo

$$u=x_1+\varepsilon x_2+\varepsilon^2x_3,\quad v=x_1+\varepsilon^2x_2+\varepsilon x_3, \tag{10}$$

veremos, que

$$\Gamma_\sigma(u)=x_{\sigma^{-1}(1)}+\varepsilon x_{\sigma^{-1}(2)}+\varepsilon^2x_{\sigma^{-1}(3)}.$$

En particular,

$$\Gamma_{(123)}(u)=x_3+\varepsilon x_1+\varepsilon^2x_2=\varepsilon u,$$
$$\Gamma_{(23)}(u)=x_1+\varepsilon x_3+\varepsilon^2x_2=v,$$
$$\Gamma_{(123)}(v)=x_3+\varepsilon^2x_1+\varepsilon x_1=\varepsilon^{-1}v,$$
$$\Gamma_{(23)}(v)=x_1+\varepsilon^2x_3+\varepsilon x_2=u,$$

o sea, las operaciones Γ_σ en u, v y σ en x_1, x_2, x_3, están coordinadas. Sustituyendo (10) en los invariantes (9) estos últimos pasan a ser funciones simétricas de x_1, x_2, x_3, las cuales, según el teorema 1, § 2, cap. 6, se pueden expresar por medio de las funciones simétricas elementales $s_i=s_i(x_1,\ x_2,\ x_3)$. Un pequeño ejercicio muestra que

$$I_1=x_1^2+x_2^2+x_3^2+(\varepsilon+\varepsilon^2)(x_1x_2+x_1x_3+x_2x_3)=s_1^2+3s_2,$$
$$I_2=2(x_1^3+x_2^3+x_3^3)-3(x_1^2x_2+x_1^2x_3+x_1x_2^2+$$
$$+x_1x_3^2+x_2^2x_3+x_2x_3^2)+12x_1x_2x_3=2s_1^3-9s_1s_2+27s_3.$$

Especifiquemos los valores de I_1, I_2 tomando como x_1, x_2, x_3 las tres raíces de la ecuación cúbica incompleta

$$x^3+px+q=0.$$

Entonces, $s_1 = 0$, $s_2 = p$, $s_3 = -q$ y, por consiguiente,

$$I_1 = -3p, \quad I_2 = -27q. \tag{11}$$

Pero, de (9) se deduce, que

$$v = \frac{I_1}{u}, \quad I_2 = u^3 + \frac{I_1^3}{u^3}, \quad u = \sqrt[3]{\frac{I_2}{2} \pm \sqrt{\frac{I_2^2}{4} - I_1^3}}.$$

Se eligen tales radicales, que luego de sustituir los valores de (11), se obtienen las fórmulas

$$u = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}, \quad v = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}, \quad uv = -3p,$$

con la magnitud $D = -4p^3 - 27q^2$, que es el discriminante de nuestra ecuación cúbica (véase (16), § 2, cap. 6). Como u y v ahora son conocidos, entonces, del sistema lineal

$$\begin{aligned} x_1 + \varepsilon x_2 + \varepsilon^2 x_3 &= u, \\ x_1 + \varepsilon^2 x_2 + \varepsilon x_3 &= v, \\ x_1 + x_2 + x_3 &= 0 \end{aligned}$$

se hallan las propias raíces. Por un camino bastante natural, llegamos a las fórmulas de Cardan, sobre las que se hizo mención en el ejercicio 1, § 2, cap. 1.

El último ejemplo establece, no casualmente, la relación entre los invariantes del grupo S_3, que es el grupo de Galois de la ecuación cúbica general, y las fórmulas de Cardan. La teoría de Galois en gran medida se vincula al estudio de invariantes de campos (y a sus grupos correspondientes), engendrados por las raíces de ecuaciones algebraicas.

Destaquemos algunos hechos, referidos a un sistema de generadores del anillo de invariantes. Sea w una forma arbitraria de n variables independientes $x_1, \ldots, x_n$. El grupo finito G con representación lineal Φ de grado n opera como grupo de permutaciones en el conjunto

$$\Omega = \{\tilde{\Phi}_g(w) \mid g \in G\}.$$

Es claro, que cualquier función simétrica homogénea $|G|$ (o, posiblemente, algún divisor del número $|G|$) de los elementos de Ω, será invariante del grupo lineal (G, Φ). Si ahora se toma en calidad de w la variable x_i, entonces, x_i será raíz de la ecuación algebraica

$$\prod_{g \in G} (X - \Phi_g(x_i)) = 0,$$

cuyos coeficientes resultan invariantes del grupo (G, Φ). De este modo, cada variable x_i es función (algebraica) de invariantes. Si el número de invariantes algebraicamente independientes fuese menor que n, expresaríamos $x_1, \ldots, x_n$ por medio de una cantidad menor de variables algebraicas independientes, pero esto es imposible. Por consiguiente, hemos demostrado (si se puede llamar demostración a un manejo tan atrevido de la dependencia de magnitudes algebraicas) uno de los teoremas importantes de la teoría de invariantes.

TEOREMA 4. *Un grupo lineal finito de grado n, siempre tiene un sistema de n invariantes algebraicamente independientes.* ∎

Para el grupo (S_3, Γ), tales invariantes son las formas (9).

Se podía completar el teorema 4 con la afirmación acerca de que todo el anillo de invariantes enteros de un grupo finito de grado n, es engendrado por n invariantes algebraicamente independientes $f_1, f_2, \ldots, f_n$ y, por lo común, otro invariante más f_{n+1} (que es función algebraica de los primeros n). Con otras palabras, los restantes invariantes, son polinomios de $f_1, \ldots, f_n, f_{n+1}$. Este hecho es cierto para muchos otros grupos lineales, tanto discretos como continuos.

La teoría general de invariantes, desarrollada a mediados del siglo XIX con los trabajos de Cayley, Silvester, Jacobi, Hermite, Klebetz, Gordan y otros, y que luego experimentó un renacimiento en algunos trabajos fundamentales de D. Hilbert, en nuestros días es parte de la geometría algebraica y de la teoría de grupos algebraicos. El interés permanente hacia la teoría de invariantes también se funda en las amplias posibilidades de sus usos en muchos dominios de la mecánica y la física.

EJERCICIOS

1. Demostrar el teorema 1, siguiendo las designaciones usadas en su formulación, y el conjunto de razonamientos expuestos a continuación.

a) Si $V = \langle e_1, \ldots, e_n\rangle_P$, $W = \langle f_1, \ldots, f_m\rangle_P$, entonces, (T1) — (T3) son equivalentes a la globalidad de una única condición: los vectores $\tau(e_i, f_j)$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$, componen la base del espacio T.

b) Para cualquier espacio nm-dimensional T sobre P, la aplicación τ se puede definir como la relación $\tau(v, w) = \sum \alpha_i\beta_j g_{ij}$; donde g_{ij}, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$, son base en T. De acuerdo con a), el par (τ, T) cumple las condiciones (T1)—(T3), y todos los pares se obtienen del mismo modo.

c) Para todo par (τ', T') con aplicación bilineal $\tau'\colon V \times W \to T'$, definimos la aplicación lineal $\sigma\colon T \to T'$, haciendo $\sigma(\sum\gamma_{ij}g_{ij}) = \sum\gamma_{ij}\tau'(e_i, f_j)$.

De acuerdo con b) y c), $\tau'(v, w) = \sum\alpha_i\beta_j\tau'(e_i, f_j) = \sigma(\sum\alpha_i\beta_j g_{ij} = \sigma(\tau(v, w))$. Y, viceversa, si $\sigma(\tau(v, w)) = \tau'(v, w)$, entonces, $\sigma(g_{ij}) = \sigma(\tau(e_i, f_j)) = \tau'(e_i, f_j)$.

2. Mostrar, que en el sistema (T1)—(T3), se puede omitir la condición (T1) o (T2), y, suponiendo a priori $\dim T = nm$, para el producto tensorial es suficiente dejar una de las tres condiciones.

3. Demostrar la relación $\det(A \otimes B) = (\det A)^m (\det B)^n$ para las matrices cuadradas A, B de órdenes n y m, respectivamente, con coeficientes complejos, empleando la posibilidad de reducirlas a la forma triangular. (*Indicación*. Existen las matrices no degeneradas C y D tales, que

$$A' = CAC^{-1} = \begin{Vmatrix} \alpha_1 & & * \\ & \ddots & \\ 0 & & \alpha_n \end{Vmatrix}, \quad B' = DBD^{-1} = \begin{Vmatrix} \beta_1 & & * \\ & \ddots & \\ 0 & & \beta_m \end{Vmatrix}.$$

Por eso,

$$A' \otimes B' = (C \otimes D)(A \otimes B)(C^{-1} \otimes D^{-1}) = (C \otimes D)(A \otimes B)(C \otimes D)^{-1}$$

es matriz triangular con coeficientes diagonales $\alpha_i\beta_j$, que serán los valores propios de la matriz $A^1 \otimes B^1$, y, por consiguiente, $A \otimes B$. Tenemos: det $(A \otimes B) = \prod_{i,j} \alpha_i\beta_j = (\prod_i \alpha_i)^m (\prod_j \beta_j)^n = (\det A)^m (\det B)^n$.)

4. Con ayuda de la fórmula (8) y las tablas del p. 1, § 2, p. 2, § 5; p. 4, § 5, comprobar, que es correcta la descomposición

$$\Phi^{(3)} \otimes \Phi^{(3)} \approx \Phi^{(1)} + \Phi^{(2)} + \Phi^{(3)}$$

para el cuadrado tensorial de la representación bidimensional $\Phi^{(3)}$ del grupo simétrico S_3 y

$$\Phi^{(5)} \otimes \Phi^{(5)} \approx \Phi^{(1)} + \Phi^{(2)} + \Phi^{(3)} + \Phi^{(4)}$$

para el cuadrado tensorial de la representación bidimensional $\Phi^{(5)}$ del grupo de cuaterniones Q^8.

5. *Representaciones del producto directo de grupos.* Sea que se tienen dos grupos G, H, con representaciones lineales (Φ, V), (Ψ, W). Entonces, haciendo

$$(\Phi \otimes \Psi)(g \cdot h) = \Phi(g) \otimes \Psi(h),$$

donde $g \cdot h$ es elemento del producto directo $G \times H$ de los grupos G, H, obligamos a $G \times H$ operar en el producto tensorial $V \otimes_{\mathbb{C}} W$; como de costumbre,

$$((\Phi(g) \otimes \Psi(h))(v \otimes w) = \Phi(g)\, v \otimes \Psi(h)\, w.$$

Comprobar, que la aplicación así definida

$$\Phi \otimes \Psi: G \otimes H \to GL(V \otimes W)$$

es representación del grupo $G \times H$ con carácter $\chi_{\Phi \times \Psi} = \chi_\Phi \chi_\Psi$. Demostrar la afirmación siguiente. Sean $\Phi^{(1)}, \ldots, \Phi^{(r)}$ (respectivamente $\Psi^{(1)}, \ldots, \Psi^{(s)}$) todas representaciones irreducibles del grupo G (respectivamente, H). Entonces, las representaciones $\Phi^{(i)} \otimes \Psi^{(j)}$ del grupo $G \times H$ son irreducibles y todas las representaciones irreducibles del grupo $G \times H$ se agotan con las representaciones $\Phi^{(i)} \otimes \Psi^{(j)}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$.

6. Las formas xy, $x^n + y^n$ son invariantes del grupo lineal bidimensional del diedro

$$(D_n, \Phi) = \left\langle \begin{Vmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{Vmatrix}, \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix} \right\rangle, \quad \varepsilon^n = 1$$

véase el ejercicio 9, § 5). Mostrar, que cualquier otro invariante del grupo (D_n, Φ) tiene la forma del polinomio de xy, $x^n + y^n$.

7. Comprobar, que el grupo de cuaterniones, examinado en su representación irreducible bidimensional, no tiene invariantes cuadráticos y cúbicos. ¿Qué se puede decir sobre las formas x^2y^2, $x^4 + y^4$?

Capítulo 9

PARA LA TEORIA DE LOS CAMPOS, ANILLOS Y MODULOS

La revisión de las estructuras algebraicas estudiadas antes, es motivada por las consideraciones siguientes. En primer lugar, parece deseable, en cierta medida, completar nuestros conocimientos sobre los campos y anillos con afirmaciones medulosas, apoyándose, donde sea necesario, en una base teórico-grupal fuerte. En segundo lugar, los resultados del capítulo 8 sobre representaciones de grupos, de un modo natural, se incluyen en la teoría general de módulos sobre los anillos, y sería una lástima no mencionar esto, aunque sea lacónicamente. El concepto fundamental de módulo es por sí mismo importante y merece ser estudiado en un aspecto mucho más amplio, pero, para esto, se recomienda al lector dirigirse a otras fuentes.

§ 1. AMPLIACIONES FINITAS DE CAMPOS

1. Elementos primitivos y grados de las ampliaciones. Si F es un campo que contiene al subcampo P, entonces, F también se llama *ampliación* del campo P (véase § 4, cap. 4). Al principio, nos limitaremos a un caso muy sencillo, cuando la ampliación $F = P(\theta)$ se obtiene del campo P con la adjunción (dentro del campo F dado) de un único elemento $\theta \in F$. Se dice, que $P(\theta)$ es *una ampliación simple* del campo P, y θ es *un elemento primitivo* de esta ampliación. Por su significado, $P(\theta)$ es el campo de relaciones del anillo entero $P[\theta]$. El elemento θ *resulta trascendente* sobre P (véase § 2, cap. 5) si, y sólo si, la ampliación $P(\theta)$ es isomorfa al campo de las fracciones racionales. Si, no obstante, θ es un elemento *algebraico*, entonces, $P(\theta) \cong P \cong [X]/(f(X))$ (véanse, (9), § 2, cap. 5 y el corolario del teorema 5, § 2, cap. 5). Aquí, $f(X)$ es un polinomio irreducible de grado $n > 0$, cuya raíz es θ. Recíprocamente, si $f \in P[X]$ es un polinomio irreducible, entonces, se construye en forma canónica un campo F (véase § 3, cap. 6), en el cual f tiene, por lo menos, una raíz θ. De la construcción se ve que F se identifica con el conjunto de elementos del tipo

$$a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}, \quad a_i \in P, \quad n = \deg f.$$

Para los elementos del anillo $P[\theta]$ esto es evidente (dividir $g(X)$ por $f(X)$ con resto y sustituir $X = \theta$); y la división en $P(\theta]$ se efectúa así: si $g(X) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$, entonces, la irreducibilidad de f conlleva la igualdad m.c.d. $(f, g) = 1$ y la existencia de los polinomios $u(X)$, $v(X)$ de grado $< n$, para los cuales $fu + gv = 1$; de aquí, $g(\theta)v(\theta) = 1$ y $1/g(\theta) = v(\theta)$.

El número n se puede considerar dimensión del espacio vectorial

$$F = \langle 1, \theta, \ldots, \theta^{n-1}\rangle_P$$

sobre P, con elementos básicos $1, \theta, \ldots, \theta^{n-1}$.

En el caso de una ampliación arbitraria $F \supset P$, también es razonable considerar F como un espacio vectorial sobre P. Su dimensión $\dim_P F$ (posiblemente, infinita) la designaremos mediante $[F : P]$ y la llamaremos *grado de ampliación* F sobre P. Si $F = P(\theta)$, entonces $[F : P]$ también se llama *potencia del elemento primitivo*. Claro está, que para el elemento trascendente $\theta \in F$, la familia $1, \theta, \theta^2, \ldots$ es linealmente independiente sobre P y $[P(\theta), P] = \infty$. Por otra parte, de lo dicho más arriba se deriva la afirmación siguiente.

TEOREMA 1. *Sea F alguna ampliación del campo P. El elemento $\theta \in F$ es algebraico sobre P si, y sólo si, $[P(\theta) : P] < \infty$. Además, la algebraicidad de θ implica la igualdad $P(\theta) = P[\theta]$.* ∎

Llamemos a $K \supset F \supset P$ *torre de dos pisos de ampliaciones*. Ella permite hablar sobre tres espacios vectoriales: K/P (K sobre P), K/F (K sobre F) y F/P (F sobre P). Sus dimensiones están enlazadas por una relación análoga a la relación de los índices de los subgrupos.

TEOREMA 2. *En la torre de ampliaciones $K \supset F \supset P$ el grado $[K : P]$ es finito si, y sólo si, son finitos los grados $[K : F]$ y $[F : P]$. Si son finitos, es cierta la relación*

$$[K : P] = [K : F]\,[F : P].$$

DEMOSTRACION. Suponiendo primero que $[K : F]$ y $[F : P]$ son finitos, elijamos una P-base $f_1, \ldots, f_m$ en F/P y una F-base $e_1, \ldots, e_n$ en K/F. Entonces, cualquier elemento $x \in K$ se escribe en la forma $x = \sum \alpha_j e_j$, con $\alpha_j \in F$. A su vez, $\alpha_j = \sum p_{ij} f_i$ con $p_{ij} \in P$. En consecuencia, $x = \sum_{i,j} p_{ij} f_i e_j$, y observamos que mn elementos $f_i e_j$ engendran linealmente K sobre P. Supongamos que existe la dependencia lineal $\sum_{i,j} p_{ij} f_i e_j = 0$ para algunos $p_{ij} \in P$. Entonces,

$$0 = \sum_{i,j} p_{ij} f_i e_j = \sum_j \Big(\sum_i p_{ij} f_i\Big) e_j \Rightarrow \sum_i p_{ij} f_i = 0 \Rightarrow p_{ij} = 0$$

para todos $i = 1, \ldots, m$; $j = 1, \ldots, n$, por cuanto $e_1, \ldots, e_n$ son linealmente independientes sobre F, y $f_1, \ldots, f_m$ lo son sobre P. Por lo tanto, los mn elementos $f_i e_j$ forman la base del espacio vectorial K/P y $[K : P] = nm = [K : F]\,[F : P]$.

Recíprocamente, la desigualdad $[K : P] < \infty$ implica el carácter finito de $[F : P]$, por cuanto F/P es un subespacio del espacio K/P. Si $\{a_1, \ldots, a_r\}$ es P-base para K, entonces, el elemento arbitrario $x \in K$ será la combinación lineal $a_1, \ldots, a_r$ con coeficientes en P

y, con más razón, con coeficientes en F. Sobre F, el número de elementos linealmente independientes entre $a_1, \ldots, a_r$, sólo puede mermar. De esta manera, $[K : F] < \infty$. ∎

COROLARIO. *Sean F una ampliación del campo P, y A un conjunto de todos los elementos de F que son algebraicos sobre P. Entonces, A es un subcampo en F, contenedor de P.*

DEMOSTRACION. Cada elemento $t \in P$ es raíz del polinomio lineal $X - t \in P[X]$, así que $P \subset A$. Sean, luego, $u, v \in A$. Entonces, según el teorema 1, tenemos $[P(u), P] < \infty$. El elemento v, algebraico sobre P, también lo será sobre $P(u)$, o sea, $[P(u, v) : P(u)] = [P(u)(v) : P(u)] < \infty$. De acuerdo con el teorema 2, $[P(u, v) : P] = [P(u, v) : P(u)][P(u) : P] < \infty$.

Como $u - v$, $uv \in P(u, v)$, entonces, nuevamente por el teorema 1, tenemos $u - v$, $uv \in A$, o sea, A es un subanillo en F. El es un campo, por cuanto $0 \neq u \in A \Rightarrow [P(u^{-1}) : P] = [P(u) : P] < \infty$. ∎

La ampliación $F \supset P$ se llama *algebraica sobre* P, si todos los elementos de F son algebraicos sobre P. Cada elemento α de la ampliación algebraica es raíz de cierto polinomio unitario (o sea, con coeficiente mayor 1) distinto de cero $f \in P[X]$, dependiente de α. Si $f(\alpha) = 0$ y $g(\alpha) \neq 0$ para cualquier $0 \neq g \in P[X]$ con $\deg g < \deg f$, entonces, $f = f_\alpha$ se llama *polinomio mínimo del elemento* α. El polinomio mínimo es irreducible sobre P, está definido unívocamente y su grado coincide con la potencia del elemento α (frecuentemente, el polinomio obtenido del mínimo multiplicado por una constante, también se llama mínimo). Todas las raíces distintas del polinomio f_α se consideran *conjugadas* con α. Más abajo, el teorema 3, explica esta terminología. Si char $P = 0$, entonces, el número de raíces diferentes coincide con $\deg f_\alpha$ (véase § 1, cap. 6). Pero, en el caso general, esto no es así (véanse los ejercicios 4 y 5).

De acuerdo con los resultados obtenidos, la ampliación $F \supset P$ de grado finito $[F : P]$ resulta *algebraica finita*, o sea, ella se obtiene de P con la adjunción de un número finito de elementos algebraicos $\alpha_1, \ldots, \alpha_m$. Recíprocamente, *toda ampliación algebraica finita $F = P(\alpha_1, \ldots, \alpha_m)$ tiene grado finito.* En efecto, $f_k(\alpha_k) = 0$, $1 \leqslant k \leqslant m$, $f_k \in P[X]$. El elemento α_k, algebraico sobre P, será, naturalmente, también algebraico sobre $P(\alpha_1, \ldots, \alpha_{k-1})$. En consecuencia, $[P(\alpha_1, \ldots, \alpha_k) : P(\alpha_1, \ldots, \alpha_{k-1}) < \infty$ y, en correspondencia con el teorema 2,

$$[F : P] = [P(\alpha_1, \ldots, \alpha_m) : P] =$$

$$= \prod_{k=1}^{m} [P(\alpha_1 \ldots \alpha_k) : P(\alpha_1, \ldots \alpha_{k-1})] < \infty. \; ∎$$

En muchos casos (en particular, cuando char $P = 0$) la ampliación algebraica finita resulta simple. En los casos considerados por

nosotros, la existencia del elemento primitivo se establece inmediatamente.

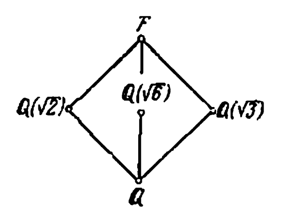
EJEMPLO. El campo $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ como espacio vectorial sobre $\mathbb{Q}$ es tetradimensional: $F = \langle 1, \sqrt{2}, \sqrt{3}, \sqrt{6}\rangle \mathbb{Q}$, o sea, cada elemento $\alpha \in F$ se escribe en forma de la combinación lineal $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ con coordenadas racionales a, b, c, d. Por otra parte, $F = \langle 1, \theta, \theta^2, \theta^3\rangle \mathbb{Q}$, donde $\theta = \sqrt{2} + \sqrt{3}$. Efectivamente, $\sqrt{2} = -\frac{9}{2}\theta + \frac{1}{2}\theta^3$, $\sqrt{3} = \frac{11}{2}\theta - \frac{1}{2}\theta^3$, $\sqrt{6} = -\frac{5}{2} + \frac{1}{2}\theta^2$. El elemento primitivo θ tiene el polinomio mínimo $f_\theta(X) = X^4 - 10X^2 + 1$ con las raíces

$\theta^{(1)} = \theta = \sqrt{2} + \sqrt{3}$, $\theta^{(2)} = \sqrt{2} - \sqrt{3}$, $\theta^{(3)} = -\sqrt{2} + \sqrt{3}$, $\theta^{(4)} = -\sqrt{2} - \sqrt{3}$.

Prestemos atención al hecho de que F es el campo de descomposición del polinomio $f_\theta(X)$, y, además

$$F = \mathbb{Q}(\theta^{(1)}, \theta^{(2)}, \theta^{(3)}, \theta^{(4)}) = \mathbb{Q}(\theta^{(i)}), \quad i = 1, 2, 3, 4.$$

En la teoría general de Galois este campo hubiese sido llamado *normal*. El diagrama de los subcampos del campo F se parece al diagrama de los subgrupos



del grupo cuaternario V_4, y esto no es casual. Si examinamos el automorfismo arbitrario $\Phi: F \to F$ (véase el p. 5, § 4, cap. 4), entonces, de las relaciones $\Phi(x + y) = \Phi(x) + \Phi(y)$, $\Phi(xy) = \Phi(x)\Phi(y)$, $\forall x, y \in F$, se deduce que Φ se determina totalmente por su operación en el elemento primitivo θ. Luego, $\Phi(a) = a$, $\forall a \in \mathbb{Q}$, por eso

$$\Phi(\theta)^4 - 10\,\Phi(\theta)^2 + 1 = \Phi(\theta^4 - 10\theta^2 + 1) = \Phi(0) = 0.$$

En consecuencia, $\Phi(\theta)$ es una de las raíces $\theta^{(i)}$, $i = 1, 2, 3, 4$, y llegamos a la conclusión, que el grupo de todos los automorfismos $\mathrm{Aut}(F/\mathbb{Q})$ también llamado *grupo de Galois* $G(F/\mathbb{Q})$, o $G(f_\theta)$, tiene el orden $4 = |F : \mathbb{Q}|$. Con exactitud hasta el isomorfismo, hay sólo dos grupos de orden 4: el cíclico Z^4 y $Z_2 \times Z_2 \cong V_4$. Los cálculos inmediatos muestran que $\mathrm{Aut}(F/\mathbb{Q}) \cong V_4$.

Es más fácil convencerse de esto, examinando la representación $\mathrm{Aut}(F/\mathbb{Q})$ por las permutaciones en el conjunto $\Omega = \{1, 2, 3, 4\}$, con cuyos elementos se numeran las raíces $\theta^{(i)}$. Si, por ejemplo, $\Phi(\theta^{(1)}) = \theta^{(2)}$, entonces, $\theta^{(1)}\theta^{(2)} = -1 \Rightarrow \theta^{(2)}\Phi(\theta^{(2)}) = -1 \Rightarrow \Phi(\theta^{(2)}) = \theta^{(1)}$ y $\Phi(\theta^{(3)}) = -\Phi(\theta^{(2)}) = -\theta^{(1)} = \theta^{(4)}$, o sea, $\Phi \approx (12)(34) = \sigma$. Análogamente se obtienen los automorfismos $(13)(24) = \tau$ y $(14)(23) = \sigma\tau$.

Falta agregar a lo dicho, que el subgrupo cíclico $\langle\sigma\rangle$ deja, de a un elemento, inmóvil el subcampo intermedio $\mathbb{Q}(\sqrt{2})$ y $\langle\sigma\rangle$ es el grupo $G(F/\mathbb{Q}(\sqrt{2}))$ de todos los automorfismos (grupo de Galois) del campo F respecto al subcampo $\mathbb{Q}(\sqrt{2})$. De un modo similar, como campos de invariantes para $\langle\tau\rangle$ y $\langle\sigma\tau\rangle$ sirven, respectivamente $\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(\sqrt{6})$, en tanto, los grupos de Galois

$G(F/\mathbb{Q}(\sqrt{3}))$, $G(F/\mathbb{Q}(\sqrt{6}))$ serán, a su vez, $\langle\tau\rangle$ y $\langle\sigma\tau\rangle$. En un ejemplo particular, hemos comprobado la veracidad de la correspondencia biyectiva de Galois entre los subcampos del campo normal F y los subcampos de sus grupos de automorfismos.

2. Isomorfismo de los campos de descomposición. En el § 3, cap. 6, donde se definió y construyó el campo de descomposición F sobre P del polinomio unitario $f(X) = X^n + a_1X^{n-1} + \ldots + a_n \in P[X]$, se observó, que en su formulación hay elementos de arbitrariedad. Repitiendo ahora esta construcción, podríamos solamente decir, que $[F : P] \leqslant n!$ (trate de comprender por qué). Pero, de hecho, todos los campos de descomposición sobre P del polinomio f dado, son isomorfos. A fin de precisar esta declaración, examinemos una situación un poco más general.

De acuerdo con el teorema 3, § 2, cap. 5, cualquier aplicación isomorfa φ del campo P en el campo $\widetilde{P}$ se continúa de un modo único hasta el isomorfismo $P[X]$ en $\widetilde{P}[X]$, así que

$$f(X)\ X^n + a_1X^{n-1} + \ldots + a_n \mapsto \widetilde{f}(X) = \varphi_X f = X^n + \varphi(a_1)X^{n-1} + \ldots + \varphi(a_n).$$

TEOREMA 3. *Sea $\varphi\colon P \mapsto \widetilde{P}$ un isomorfismo de campos; $f \in P[X]$ un polinomio unitario de grado $n > 0$; $\widetilde{f} = \varphi f$ su imagen para el isomorfismo φ_X: F, $\widetilde{F}$ los campos de descomposición de los polinomios, f, $\widetilde{f}$, sobre P y $\widetilde{P}$, respectivamente. Entonces, φ se continúa hasta el isomorfismo $\Phi : \widetilde{F} \mapsto F$ por $k \leqslant [F : P]$ procedimientos, además, $k = [F : P]$, si todas las raíces del polinomio $f(X)$ son diferentes.*

DEMOSTRACION. ETAPA I. Primeramente consideremos el caso de ampliaciones arbitrarias $K \supset P$, $\widetilde{K} \supset \widetilde{P}$. Sea $\theta \in K$ un elemento algebraico con polinomios mínimo $g = g_\theta \in P[X]$. Se afirma que el isomorfismo $\varphi\colon \widetilde{P} \to P$ se continúa hasta el monomorfismo ρ: $P(\theta) \to \widetilde{K}$ exactamente cuando $\widetilde{g}$ tiene raíz en $\widetilde{K}$, además, el número de continuaciones coincide con el número de diferentes raíces $\widetilde{g}$ en $\widetilde{K}$.

Efectivamente, de la existencia de ρ se deduce que el elemento $\rho(\theta)$ debe ser raíz $\widetilde{g}$: $g(\theta) = 0 \Rightarrow \widetilde{g}(\rho(\theta)) = \rho(g(\theta)) = 0$. Recíprocamente, si $g(\omega) = 0$, entonces, $\operatorname{Ker}\psi \supset g(X)P[X]$, donde $\psi\colon P[X] \to \widetilde{K}$ es un homomorfismo, determinado por la correspondencia $u(X) \to \widetilde{u}(\omega)$. Como en el caso de los grupos, ψ induce el homomorfismo $\overline{\psi}\colon P[X]/g(X)P[X] \to \widetilde{K}$ $(u(X) + g(X)P[X] \mapsto \widetilde{u}(\omega)$: si esto no es del todo claro, entonces, hay que dirigirse a

los resultados del siguiente § 2). Notemos, que en virtud de la irreducibilidad de $g(X)$, el anillo cociente $P[X]/g(X)P[X]$ es un campo, así que ψ resulta un monomorfismo. Exactamente del mismo modo se determina el isomorfismo de los campos $\bar{\sigma}$: $P[X]/g(X) \times \times P[X] \to P(\theta)$ $(u(X) + g(X)P[X] \mapsto u(\theta))$. La composición $\rho = \bar{\psi} \circ \bar{\sigma}^{-1}$ es monomorfismo de la aplicación $P(\theta)$ en $\tilde{K}$ $(\rho(u(\theta)) = = \tilde{u}(\omega))$. Como $P(\theta)$ es engendrado sobre P por el elemento θ, entonces, ρ es la única continuación de φ, que traslada θ a ω. Esto significa precisamente que el número de isomorfismos distintos ρ con limitación $\rho|_P = \varphi$ es igual al número de raíces diferentes $\tilde{g}(X)$ en $\tilde{K}$.

ETAPA II. El campo de descomposición se construyó mediante la adjunción sucesiva de las raíces de polinomios irreducibles. Utilicemos a continuación la inducción sobre la dimensión de $[F : P]$.

Para $[F : P] = 1$, el polinomio f se descompone en factores lineales ya en $P[X] : f(X) = (X - c_1) \ldots (X - c_n)$. En tal caso, $\tilde{f}(X) = (\varphi_X f)(X) = (X - \tilde{c}_1) \ldots (X - \tilde{c}_n)$. Las raíces $\tilde{c}_1, \ldots, \tilde{c}_n$ del polinomio $\tilde{f}$ están contenidas en $\tilde{P}$, y, por cuanto $\tilde{F}$ es engendrado por ellas sobre $\tilde{P}$, entonces, $\tilde{F} = \tilde{P}$, así que $\Phi = \varphi_X$ es la única continuación.

Para $[F : P] > 1$ descompongamos $f(X)$ sobre P en factores irreducibles unitarios, entre los cuales debe hacer por lo menos un polinomio de grado $m > 1$. Designémoslo por $g(X)$. Puesto que

$$f(X) = g(X)h(X) \Rightarrow \tilde{f}(X) = (\varphi_X f)(X) = \tilde{g}(X)\tilde{h}(X),$$

entonces, sobre los campos de descomposición F y $\tilde{F}$ tienen lugar las descomposiciones de los polinomios

$$g(X) = (X - \theta_1) \ldots (X - \theta_m),$$

$$\tilde{g}(X) = (X - \omega_1) \ldots (X - \omega_m), \quad m \leqslant n.$$

En virtud de su irreducibilidad, $g(X)$ es el polinomio mínimo del elemento θ_1 sobre P y $[P(\theta_1) : P] = m$.

Si entre $\omega_1, \ldots, \omega_m$ se tienen l distintos, entonces, de acuerdo con la etapa 1, existirán l aplicaciones monomorfas $\rho_1, \ldots, \rho_l$ de la ampliación $L = P(\theta_1)$ en $\tilde{F}$ con $\rho_i|_P = \varphi$. La estructura del campo de descomposición es tal, que F puede ser considerado campo de descomposición sobre L del polinomio $f \in L[X]$, y $\tilde{F}$ se puede interpretar como campo de descomposición sobre $\rho_i(L)$ del polinomio $\tilde{f}(X)$, para cualquier $i = 1, 2, \ldots, l$. Según el teorema 2, tenemos la desigualdad $[F : L] = [F : P]/m < [F : P]$, así que, por presupuesto de la inducción, cada uno de los ρ_i se puede conti-

nuar hasta el isomorfismo $\Phi_{i,j}$: $F \to \tilde{F}$, además, el número de tales continuaciones (de índices j) no supera $[F : L]$, siendo igual a este límite superior, si todas las raíces en $\tilde{F}$ del polinomio $\tilde{f}$ son diferentes. Como $\Phi_{i,j} \mid_L = \rho_i$, $1 \leqslant j \leqslant [F : L]$, y $\rho_i \mid_P = \varphi$, entonces, $\Phi_{i,j}$ es la continuación de φ, además, $\rho_i \neq \rho_s \Rightarrow \Phi_{i,j} \neq \Phi_{s,t}$, cuando $i \neq s$. Por consiguiente, en total se obtienen $k \leqslant m\,[F : L] = [F : P]$ continuaciones del isomorfismo φ. Esta desigualdad pasa a ser igualdad, si todas las raíces de $\tilde{f}$ son distintas.

ETAPA III. Sea, finalmente, $\Phi : F \to \tilde{F}$ una continuación arbitraria de φ. Al aigual que en la etapa II, la limitación $\Phi \mid_L$, al ser aplicación monomorfa de L en $\tilde{F}$, coincide con uno de los ρ_i, y, en tal caso, Φ coincide con uno de los $\Phi_{i,j}$. ∎

COROLARIO 1. *Cualesquiera dos campos de descomposición F, $\tilde{F}$ sobre P del polinomio $f \in P[X]$ son isomorfos.*

En efecto, es suficiente hacer $\tilde{P} = P$ en el teorema 3 y tomar en calidad de φ la aplicación unitaria de P en sí mismo. ∎

COROLARIO 2. *El grupo de automorfismos* Aut (F/P) *de cualquier campo de descomposición F sobre P del polinomio $f \in P[X]$ es finito y de orden $\leqslant [F : P]$. Si todas las raíces del polinomio $f(X)$ son diferentes, entonces,* $|\operatorname{Aut}(F/P)| = [F : P]$.

La demostración se deduce inmediatamente del teorema 3.

OBSERVACION. Aunque el campo de descomposición F sobre $\mathbb{Q}$ (o sobre cualquier otro campo numérico) del polinomio $f \in \mathbb{Q}[X]$ se puede considerar incluido en el campo $\mathbb{C}$ de los números complejos, y por lo tanto, determinado unívocamente, el corolario 2 muestra, que en este caso, tendría sentido analizar la poco agradable demostración del teorema 3.

3. Campos finitos. Además de $Z_p = \mathbb{Z}/p\mathbb{Z}$, nos hemos encontrado con otros ejemplos de campos finitos (véase el § 4, cap. 4). Ha llegado el momento de incluirlos en la teoría general.

La primera observación evidente, se refiere a la ampliación arbitraria finita $K \supset F$ del campo finito F: *si $|F| = q$ y $[K : F] = n$, entonces, $|K| = q^n$.* Efectivamente, después de elegir la base del espacio vectorial K/F, el último se identifica con el espacio F^n de las filas $(\alpha_1, \ldots, \alpha_n)$ de longitud n. Todas las coordenadas α_i, independientemente unas de otras, toman q valores de F. Por lo tanto, $|K| = |F^n| = q^n$. ∎

La segunda observación, vinculada con la primera, consiste en que, *cualquier campo finito F tiene una característica finita p (p es un número primo) y $|F|$ es la potencia de p.* En efecto, el subcampo simple $P \subset F$, en virtud de la finitud de F, debe ser isomorfo a cierto campo $Z_p = \mathbb{Z}/p\mathbb{Z}$. De acuerdo con la primera observación,

la ampliación finita $F \supset P$ con $|P| = p$, tiene una potencia $|F| = p^m$.

TEOREMA 4. *Para cada campo finito F y para cada número entero positivo n, existe una, y, con exactitud hasta el isomorfismo, sólo una ampliación $K \supset F$ de grado $[K : F] = n$.*

DEMOSTRACION A) UNICIDAD. Sea $K \supset F$, una ampliación de grado n. Como sabemos, $|F| = q \Rightarrow q = p^m$, p es primo y $|K| = q^n$. En consecuencia, el grupo multiplicativo $K^* = K \setminus \{0\}$ tiene el orden $q^n - 1$, y el orden de cada uno de sus elementos, según el teorema de Lagrange, divide a $q^n - 1 : t^{q^n - 1} = 1$, $\forall t \neq 0$. Esto significa, que todos los elementos del campo K (incluyendo $t = 0$) son raíces diferentes del polinomio $X^{q^n} - X$, y tiene lugar la descomposición

$$X^{q^n} - X = \prod_{t \in K} (X - t).$$

Sobre ningún subcampo propio del campo K con un número de elementos $< q^n$ una descomposición así en factores lineales es posible, por eso, K es el campo de descomposición del polinomio $X^{q^n} - X$. Recurriendo al corolario 1 del teorema 3, llegamos a la conclusión requerida.

B) EXISTENCIA. Los razonamientos de la parte a), dictan el camino posible de construcción de K. Tomemos como K el campo de descomposición sobre $P \cong Z_p$ del polinomio $f(X) = X^{q^n} - X$. Como $q = p^m$, entonces, $q \cdot 1 = 0$ en K. Por esta razón, $f'(X) = q^n \cdot 1 \cdot X^{q^n - 1} - 1 = -1$ y, por el criterio conocido (teorema 4, § 1, cap. 6), $f(X)$ no tiene raíces múltiples. Esto quiere decir, que el subconjunto $K_f \subset K$ de las raíces del polinomio $f(X)$ tiene una potencia $|K_f| = q^n$.

Como $K_f \subset K$ y char $K = p$, entonces, conforme al ejercicio 8, § 4, cap. 4, $(x + y)^{p^s} = x^{p^s} + y^{p^s}$, para cualesquiera $x, y \in K_f$ $(F \subset K_f)$ y $s = 0, 1, 2, \ldots$ En particular,

$$x, y \in K_f \Rightarrow (x \pm y)^{q^n} = x^{q^n} \pm y^{q^n} = x \pm y \Rightarrow x \pm y \in K_f.$$

Además,

$$1 \in K_f; \ (xy)^{q^n} = x^{q^n} y^{q^n} = xy \Rightarrow xy \in K_f;$$

$$0 \neq x \in K_f \Rightarrow (x^{-1})^{q^n} = x^{-1} \Rightarrow x^{-1} \in K_f.$$

De este modo, K_f es un subcampo en K, contenedor de F y de todas las raíces del polinomio $f(X)$. En correspondencia con la definición de campo de descomposición deberá cumplirse la igualdad $K_f = K$. El grado de $[K : F]$ es igual a n, por cuanto $q^{[K:F]} = |K| = |K_f| = q^n$. ∎

COROLARIO. *Para cada número primo p y para cada número entero positivo n, existe un, y, con exactitud hasta el isomorfismo, sólo un campo con un número de elementos* p^n.

La demostración consiste en aplicar el teorema 4 al caso particular de $|F| = p$. ∎

Como ya fue señalado en el § 4, cap. 4, el campo finito con $q = p^n$ elementos, es habitual designarlo con el símbolo $\mathbb{F}_q$ o, en honor de E. Galois, con el símbolo $GF(p^n)$. Establezcamos una serie de propiedades de los campos finitos.

TEOREMA 5. *Son correctas las afirmaciones siguientes.*

(i) *El grupo multiplicativo* $\mathbb{F}_q^*$ *del campo finito* $\mathbb{F}_q$, *es un grupo cíclico de orden* $q - 1$.

(ii) *El grupo de automorfismos* Aut $(\mathbb{F}_q)$ del *campo finito* $\mathbb{F}_q$ *con un número de elementos* $q = p^n$, *es cíclico de orden* n, *además,*

$$\text{Aut}\,(\mathbb{F}_q) = \langle \Phi \mid \Phi(t) = t^p, \quad \forall t \in \mathbb{F}_q\rangle.$$

(iii) *Si* $\mathbb{F}_{p^d}$ *es un subcampo del campo* $\mathbb{F}_{p^n}$, *entonces,* $d \mid n$. *Recíprocamente, a cada divisor d del número n, le corresponde exactamente un subcampo* $\{t \in \mathbb{F}_{p^n} \mid \Phi^d(t) = t\} = \mathbb{F}_{p^d}$. *Los automorfismos que dejan este subcampo inmóvil de a un elemento, generan el grupo* Aut $(\mathbb{F}_{p^n}/\mathbb{F}_{p^d}) = \langle \Phi^d \rangle$. *De este modo, se tiene una correspondencia biyectiva entre los subcampos del campo finito* $\mathbb{F}_q$ *y los subgrupos de su grupo de automorfismos (correspondencia de Galois).*

(iv) *Si* $q = p^n$ y $\mathbb{F}_q^* = \langle \theta \rangle$, *entonces,* θ *es elemento primitivo del campo con polinomio mínimo* $h(X)$ *de grado n.* $\mathbb{F}_q$ *es el campo de descomposición sobre* $\mathbb{F}_p$ *del polinomio* $h(X)$.

(v) *Para cualquier número natural m, existe por lo menos un polinomio irreducible de grado m, sobre* $\mathbb{F}_q$.

DEMOSTRACION. (i) Demostremos una afirmación más general. Sean, F un campo arbitrario y A un subgrupo finito del grupo multiplicativo F^*. Al grupo abeliano finito A le son aplicables los resultados del § 5, cap. 7. En particular, sabemos que el carácter cíclico de A es equivalente a la coincidencia del orden $|A|$ con el índice m del grupo A, el menor número natural para el cual $a^m = 1$, $\forall a \in A$. Para $m < |A|$, el polinomio $X^m - 1$ tendría en F más de m raíces, lo que es imposible. En consecuencia, el grupo A es cíclico.

(ii) Consideraremos a $\mathbb{F}_q$ como si fuera una ampliación finita $\mathbb{F}_q \supset \mathbb{F}_p$ de grado n de su subcampo simple $\mathbb{F}_p \cong Z_p$. Como $\mathbb{F}_q$ es el campo de descomposición del polinomio $X^q - X$, que tiene todas las raíces diferentes, entonces, de acuerdo con el corolario 2 del teorema 3, $|\text{Aut}\,(\mathbb{F}_q)| = n$. De las relaciones $(x + y)^p = x^p + y^p$, $(xy)^p = x^p y^p$, $1^p = 1$, señaladas en el transcurso de la demostración del teorema 4, se observa, que la aplicación $\Phi: t \mapsto t^p$ es automorfismo del campo $\mathbb{F}_q$ (la finitud de $\mathbb{F}_q$ es esencial). Si $\Phi^s: t \mapsto t^{p^s}$ es

el automorfismo unidad, entonces, $t^{p^s} - t = 0$ para todo $t \in \mathbb{F}_q$, de donde se deduce la desigualdad $s \geqslant n$. Pero, cuando $s = n$, realmente obtenemos el automorfismo unidad, así que $|\langle\Phi\rangle| = n$ y $\langle\Phi\rangle = \mathrm{Aut}(\mathbb{F}_q)$.

(iii) De acuerdo con la primera observación sobre los campos finitos (véase el principio del punto), $p^n = (p^d)^r$, donde r es el grado de la ampliación $\mathbb{F}_{p^n} \supset \mathbb{F}_{p^d}$. Por eso, $n = dr$. Recíprocamente, para cualquier $d \mid n$ introduzcamos el subconjunto $F = \{t \in \mathbb{F}_{p^n} \mid t^{p^d} = t\}$. Como $n = dr \Rightarrow p^n - 1 = (p^d)^r - 1 = (p^d - 1)s$, entonces

$$X^{p^n} - 1 = X^{(p^d-1)s} - 1 = (X^{p^d-1} - 1)\, g(X),$$

$$X^{p^n} - X = (X^{p^d} - X)\, g(X).$$

Como $\mathbb{F}_{p^n}$ es el campo de descomposición del polinomio $X^{p^n} - X$, entonces, exactamente p^d elementos de $\mathbb{F}_{p^n}$ serán raíces del polinomio $X^{p^d} - X$. Precisamente, de ellas se compone el subconjunto F, que ahora se puede identificar con $\mathbb{F}_{p^d}$. Con este razonamiento dual al teorema 4, también se establece la unicidad del subcampo con p^d elementos.

Observemos, que, por construcción,

$$\mathbb{F}_{p^d} = \{t \in \mathbb{F}_{p^n} \mid \Phi^d(t) = t\}$$

es el conjunto de todos los elementos que quedan en su lugar, con la operación $\langle\Phi^d\rangle$. Como el grupo $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\Phi\rangle$ es cíclico, inmediatamente se ve, que cualquier automorfismo Φ^l, no perteneciente a $\langle\Phi^d\rangle$, opera en $\mathbb{F}_{p^d}$ de varios modos (es suficiente aplicar Φ^l al generador del grupo $\mathbb{F}_{p^d}^*$). Esto significa, que el grupo de automorfismos relativos $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})$ coincide con $\langle\Phi^d\rangle$. En la afirmación (iii), la frase final tiene el mismo sentido que en el ejemplo del punto 1.

(iv) Es completamente evidente, que $\mathbb{F}_q = \mathbb{F}_p(\theta)$, $q = p^n$. Sea $h(X) = X^n + a_1X^{n-1} + \ldots + a_n$ el polinomio mínimo del elemento primitivo θ. Como los elementos del subcampo simple $\mathbb{F}_p$ son inmóviles para todos los automorfismos, y $a_i \in \mathbb{F}_p$, entonces, por lo tanto, $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$, son las raíces de $h(X)$. Todas ellas están contenidas en nuestro campo y $\mathbb{F}_p(\theta, \ldots, \theta^{p^{n-1}}) = \mathbb{F}_p(\theta) = \mathbb{F}_{p^n}$ es el campo de descomposición del polinomio $h(X)$ sobre $\mathbb{F}_p$.

(v) Apoyándonos en el teorema 4, construyamos la ampliación $K \supset \mathbb{F}_q$ de grado m. Según (i), K^* es un grupo cíclico. Si $K^* = \langle\theta\rangle$ y $h(X)$ el polinomio mínimo del elemento primitivo θ, entonces, $K = \mathbb{F}_q(\theta)$ y $\deg h(X) = [\mathbb{F}_q(\theta) : \mathbb{F}_q] = [K : \mathbb{F}_q] = m$. El polinomio mínimo, por definición, es irreducible (sobre $\mathbb{F}_q$), por eso, tenemos todo lo necesario. ∎

Luego de sencillas preparaciones teórico-numéricas, obtendremos una fórmula exacta para el número de polinomios irreducibles de grado m, sobre $\mathbb{F}_q$.

4. Fórmula de revolución de Möbius y sus usos. La función teórico-numérica μ, definida por las reglas

$$\mu(n) = \begin{cases} 1, & \text{si } n = 1, \\ (-1)^k, & \text{si } n = p_1 \ldots p_k,\ p_i \text{ son primos diferentes}, \\ 0, & \text{si } n \text{ se divide por un cuadrado} > 1, \end{cases}$$

se llama *función de Möbius*. Es claro, que μ es una *función multiplicativa*, en el sentido, que μ no es idénticamente igual a cero, y que $\mu(nm) = \mu(n)\mu(m)$ para cualesquiera n y m primos entre sí. También es claro, que si $n = p_1^{m_1} \ldots p_r^{m_r}$, entonces, $\sum_{d|n} \mu(d) = \sum_{d|n_0} \mu(d)$, donde $n_0 = p_1 \ldots p_r$ es el divisor máximo de n, libre de cuadrados. A su vez, el número de divisores $d = p_{i_1} \ldots p_{i_s}$ del número n_0 con s fijo, es igual a $\binom{r}{s}$. De este modo para $n > 1$, tenemos

$$\sum_{d|n} \mu(d) = \sum_{d|n_0} \mu(d) = \sum_{s=0}^{r} \binom{r}{s} (-1)^s = (1-1)^r = 0$$

(la suma en la parte izquierda se efectúa por todos los divisores $d \geqslant 1$ del número entero n). Definitivamente, obtenemos la fórmula

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{si } n = 1, \\ 0, & \text{si } n > 1, \end{cases} \tag{1}$$

Es también útil su modificación

$$\sum_{d|n|m} \mu\left(\frac{m}{n}\right) = \begin{cases} 1, & \text{si } d = m; \\ 0, & \text{si } d|m,\ d < m \end{cases} \tag{2}$$

(se suma con respecto a n, divisor de m y divisible por d). Haciendo $m = dt$, $n = dl$ y obligando a l recorrer los divisores del número t, fácilmente pasamos de (2) a (1) y viceversa.

La fórmula (1) (o la (2)) se podía haber tomado como definición de la función de Möbius por inducción. Para nosotros, su valor consiste en la siguiente afirmación. *Sean f y g dos funciones arbitrarias de* $\mathbb{N}$ *en* M ($M = \mathbb{Z}, \mathbb{R}, F[X]$, etc.), *vinculadas por la relación*

$$f(n) = \sum_{d/n} g(d). \tag{3}$$

Entonces,

$$g(n)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)f(d). \tag{4}$$

En efecto, teniendo en cuenta (2), la suma inmediata con respecto a n, divisor de m, de ambos miembros de (3) multiplicados por $\mu\left(\frac{m}{n}\right)$, da

$$\sum_{n\mid m}\mu\left(\frac{m}{n}\right)f(n)=\sum_{n\mid m}\mu\left(\frac{m}{n}\right)\cdot\sum_{d\mid n}g(d)=$$

$$=\sum_{d\mid m}g(d)\cdot\sum_{d\mid n\mid m}\mu\left(\frac{m}{n}\right)=g(m).$$

Un sencillo cambio de designaciones lleva a la fórmula (4), llamada *fórmula de revolución de Möbius*. Análogamente se realiza el paso de (4) a (3). ∎

También se tiene un análogo multiplicativo de la fórmula de revolución de Möbius. *Si*

$$f(n)=\prod_{d\mid n}g(d),$$

entonces,

$$g(n)=\prod_{d\mid n}f(d)^{\mu\left(\frac{n}{d}\right)}, \tag{5}$$

Para la demostración es necesario realizar los mismos cálculos formales:

$$\prod_{n\mid m}f(n)^{\mu\left(\frac{m}{n}\right)}=\prod_{n\mid m}\prod_{d\mid n}g(d)^{\mu\left(\frac{m}{n}\right)}=$$

$$\prod_{d\mid m}\prod_{d\mid n\mid m}g(d)^{\mu\left(\frac{m}{n}\right)}=\prod_{d\mid m}g(d)^{\sum\limits_{d\mid n\mid m}\mu\left(\frac{m}{n}\right)}=g(m),$$

y luego modificar levemente las designaciones.

Pongamos tres ejemplos de uso de la fórmula de revolución de Möbius.

EJEMPLO 1 (*la función φ de Euler*). Por definición, $\varphi(n)$ es el número de magnitudes primas entre sí con n números de la serie $0, 1, \ldots$ $\ldots, n-1$, o, lo que es equivalente, $\varphi(n)=|U(Z_n)|$ es el orden del grupo de los elementos invertibles del anillo $Z_n=\mathbb{Z}/n\mathbb{Z}$. Del ejercicio 5, § 1, cap. 8 conocemos la relación

$$n=\sum_{d\mid n}\varphi(d). \tag{6}$$

Inmediatamente, según la fórmula (4), obtenemos

$$\varphi(n)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)d=\sum_{d\mid n}(\mu)\,d\,\frac{n}{d}=n\sum_{d\mid n}\frac{\mu(d)}{d}.$$

Si $n=p_m^{m_1}\dots p_r^{m_r}$, entonces

$$\sum_{d\mid n}\frac{\mu(d)}{d}=1-\sum_i\frac{1}{p_i}+\sum_{i<j}\frac{1}{p_ip_j}-\dots+(-1)^r\frac{1}{p_1p_2\dots p_r}=$$

$$=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right).$$

De este modo,

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(\frac{1}{p_r}\right)$$

es la fórmula que ya mostramos en el ejercicio 3, § 8, cap. 1, y de la cual se deduce inmediatamente la multiplicatividad de la función φ.

EJEMPLO 2 (*polinomios circulares*). El campo de descomposición Γ_n sobre $\mathbb{Q}$ del polinomio X^n-1, se llama *circular o ciclotómico*. Como todas las raíces de potencia n de 1 forman un grupo cíclico de orden n, entonces, el campo circular tiene la forma $\Gamma_n=\mathbb{Q}(\zeta)$, donde ζ es una de las raíces primitivas ($\zeta\in\mathbb{C}$). Desearíamos hallar el grado de $[\Gamma_n:\mathbb{Q}]$ y el polinomio mínimo del elemento ζ sobre $\mathbb{Q}$.

Designemos con el símbolo P_n el conjunto de potencia $|P_n|=\varphi(n)$ de raíces primitivas de potencia n de 1. Los subgrupos del grupo cíclico de orden n se encuentran en relación biyectiva con los divisores d del número n (teorema 6, § 3, cap. 4), y cada raíz ζ^i se encuentra en algún conjunto P_d. Por eso, tiene lugar la participación en las clases disjuntas:

$$\{1,\ \zeta,\ \zeta^2,\ \dots,\ \zeta^{n-1}\}=\bigcup_{d\mid n}P_d \tag{7}$$

(pasando a potencias de conjuntos, llegaríamos de nuevo a la relación (6)). El polinomio

$$\Phi_n(X)=\prod_{\varepsilon\in P_n}(X-\varepsilon)$$

de grado $\varphi(n)$, se llama *polinomio circular* que corresponde a Γ_n. De acuerdo con la partición (7), llegamos a la descomposición

$$X^n-1=\prod_{i=0}^{n-1}(X-\zeta^i=\prod_{d\mid n}\{\prod_{\varepsilon\in P_d}(X-\varepsilon)\}=\prod_{d\mid n}\Phi_d(X). \tag{8}$$

Empleando en (8) la fórmula multiplicativa de revolución de Möbius (5), obtenemos una expresión explícita para Φ_n

$$\Phi_n(X)=\prod_{d\mid n}(X^d-1)^{\mu\left(\frac{n}{d}\right)}. \tag{9}$$

Para valores pequeños de n, tenemos

$$\Phi_1(X) = X - 1,\ \Phi_2(X) = X + 1,\ \Phi_3(X) = X + X + 1,$$
$$\Phi_4(X) = X^2 + 1,\ \Phi_6(X) = X^2 - X + 1,\ \Phi_8(X) = X^4 + 1,$$
$$\Phi_9(X) = X^6 + X^3 + 1,\ \Phi_{10}(X) = X^4 - X^3 + X^2 - X + 1,$$
$$\Phi_{12}(X) = X^4 - X^2 + 1.$$

Observemos, que

$$\Phi_n(X) \in \mathbb{Z}[X] \text{ y } \Phi_n(0) = 1. \qquad (10)$$

Para llegar a (10) se puede, obviando (9), operar por inducción. Para n pequeños esto está comprobado, y más adelante razonamos del modo siguiente. Considerando que

$$g(X) = \prod_{d \mid n,\ d \neq n} \Phi_d(X)$$

es un polinomio unitario con coeficientes numéricos enteros, y utilizando el algoritmo de división con resto (teorema 5, § 2, cap. 5), obtenemos los polinomios unívocamente determinados $q, r \in \mathbb{Z}[X]$ tales, que $X^n - 1 = q(X)g(X) + r(X)$, $\deg r(X) < \deg g(X)$. Pero, $X^n - 1 = \Phi_n(X)g(X)$ en $\mathbb{Q}[X]$, y vemos, que $\Phi_n(X) = q(X) \in \mathbb{Z}[X]$, además, la unitariedad de $g(X)$ implica la de $\Phi_n(X)$.

Es correcto el teorema acerca de que $\Phi_n(X)$ es un *polinomio irreducible sobre* $\mathbb{Q}$ *y, por lo tanto,* $\Gamma_n = \mathbb{Q}(\zeta)$ *es una ampliación de grado* $\varphi(n)$ *con polinomio mínimo* $\Phi_n(X)$ para ζ. No demostraremos esto, sólo recordaremos, que al final del § 3, cap. 5 fue establecida la irreducibilidad $\Phi_p(X) = (X^p - 1)/(X - 1) = X^{p-1} + X^{p-2} + \ldots$ $\ldots + 1$, donde p es un número primo arbitrario.

Cabe señalar, que los campos circulares, que desempeñaron un papel importante en la historia del desarrollo de la teoría de los números algebraicos, aún hoy llaman la atención de los investigadores.

EJEMPLO 3 (*polinomios irreducibles sobre* $\mathbb{F}_q$). Sea $\Psi_d(q)$ el número total de polinomios unitarios irreducibles de grado d sobre $\mathbb{F}_d$, $q = p^n$, y sea $f(X)$ uno de estos polinomios. Su campo de descomposición sobre $\mathbb{F}_q$ es isomorfo al anillo cociente $\mathbb{F}_q[X]/f(X)\mathbb{F}_q[X]$, y al campo de descomposición del polinomio $X^{q^d} - X$ (corolario del teorema 4). La existencia de la raíz común θ en los polinomios $X^{q^d} - X$ y $f(X)$ conlleva, en virtud de la irreducibilidad de $f(X)$, la divisibilidad de $X^{q^d} - X$ por $f(X)$. Como $X^{q^d} - X$ es divisor del polinomio $X^{q^m} - X$ para cualquier $m = rd$, y como $X^{q^m} - X$ no tiene raíces múltiples, entonces, llegamos a la conclusión, de que en la descomposición de $X^{q^m} - X$ sobre $\mathbb{F}_q$ entran todos los polinomios unitarios irreducibles

$$f_{d,1}(X),\ f_{d,2}(X),\ \ldots,\ f_{d,\ \Psi_d(q)}(X)$$

de cualquier grado $d \mid m$, además, exactamente una vez cada uno:

$$X^{q^m} - X = \prod_{d \mid m} \{ \prod_{k=1}^{\Psi_d(q)} f_{d,k}(X) \}. \quad (11)$$

El cálculo de los grados de los polinomios que se encuentran en ambos miembros de la igualdad (11), nos conduce a la relación

$$q^m = \sum_{d \mid m} d\Psi_d(q),$$

de la que, con el empleo directo de la fórmula de revolución de Möbius (4), se obtiene la expresión para $\Psi_m(q)$:

$$\Psi_m(q) = \frac{1}{m} \sum_{d \mid m} \mu\left(\frac{m}{d}\right) q^d. \quad (12)$$

Sea, por ejemplo, $q = 2$. Entonces,

$$\Psi_2(2) = \frac{1}{2}(2^2 - 2) = 1, \quad \Psi_3(2) = \frac{1}{3}(2^3 - 2) = 2,$$

$$\Psi_4(2) = \frac{1}{4}(2^4 - 2^2) = 3, \quad \Psi_5(2) = \frac{1}{5}(2^5 - 2) = 6,$$

$$\Psi_6(2) = \frac{1}{6}(2^6 - 2^3 - 2^2 + 2) = 9$$

(comparar con el ejercicio 10, § 1, cap. 6). La fórmula (12) muestra que, con probabilidad cercana a $1/m$, el polinomio unitario de grado m sobre $\mathbb{F}_q$, elegido arbitrariamente, resulta irreducible. Sin embargo, no hay criterios satisfactorios de irreducibilidad de un polinomio concretamente tomado. ¿Qué se puede decir, por ejemplo, sobre la irreducibilidad del trinomio $X^m + X^k + 1$ sobre $\mathbb{F}_2$? Cuestiones de tal género constantemente surgen en la teoría algebraica de codificación (problema 3, § 2, cap. 1) y al construir sucesiones seudoaleatorias.

EJEMPLO 4 *(construcciones con regla y compás)*. Sea $P \subset CS$ (véase el ejemplo 2, § 1, cap. 5) un campo numérico constructivo, que es una ampliación finita del campo $\mathbb{Q}$. Supongamos inicialmente que P es sólo real, es decir, todos sus elementos son números reales. En particular, el elemento primitivo $\theta \in P$ es un número real (véase el ejercicio 13), que puede ser construido (como longitud de un segmento) en un número finito de pasos con ayuda de la regla y el compás. Esto significa que θ es elemento del campo

$$\mathbb{Q}(\theta_1, \theta_2, \ldots, \theta_r), \text{ además, } [\mathbb{Q}(\theta_1, \ldots, \theta_k) : \mathbb{Q}(\theta_1, \ldots, \theta_{k-1})] \leqslant 2.$$

Esto último es comprensible, por cuanto θ_k es solución de las ecuaciones con coeficientes en $\mathbb{Q}(\theta_1, \ldots, \theta_{k-1})$ para dos rectas, para

una recta y una circunferencia, o para dos circunferencias. Los resultados del punto 1 sobre las potencias de las ampliaciones algebraicas, muestran que $[\mathbb{Q}(\theta_1, \ldots, \theta_r)\ \mathbb{Q}] = 2^m$, donde $m \leqslant r$. Como $\mathbb{Q}(\theta) \subset \mathbb{Q}(\theta_1, \ldots, \theta_r)$, entonces, por el teorema 2 tenemos $[\mathbb{Q}(\theta)\ \mathbb{Q}]$ = potencia de dos.

Regresando al P arbitrario (no necesariamente real), también lo escribimos en forma de $P = \mathbb{Q}(\theta)$. Ahora el elemento primitivo $\theta = a + ib$ es un número complejo con componentes constructivos reales a, b. Si $f(X)$ es el polinomio mínimo (con coeficientes racionales) para θ, entonces, $f(\theta) = 0$ y $f(\bar{\theta}) = 0$, donde $\bar{\theta} = a - ib$. Está claro que $\mathbb{Q}(\theta, \bar{\theta})$ es una ampliación algebraica finita del campo $\mathbb{Q}$. Sus elementos $a(\theta + \bar{\theta})/2$ e $ib = (\theta - \bar{\theta})/2$ son algebraicos sobre $\mathbb{Q}$; también es algebraico el elemento $b = ib/2$ (véase el corolario del teorema 2), por cuanto $i^2 + 1 = 0$.

De este modo, $\mathbb{Q}(a, b)$ es una ampliación algebraica finita real del campo $\mathbb{Q}$ con elementos constructivos a, b. De acuerdo con lo precedente $[\mathbb{Q}(a, b) : \mathbb{Q}] = 2^m$. La irreducibilidad de $x^2 + 1$ sobre $\mathbb{Q}(a, b) \subset \mathbb{R}$, significa que $[\mathbb{Q}(a, b)(i) : \mathbb{Q}(a, b)] = 2$ y $[\mathbb{Q}(a, b)(i) : \mathbb{Q}] = 2^{m+1}$. Como $P = \mathbb{Q}(\theta) \subset \mathbb{Q}(a, b, i)$, entonces $[\mathbb{Q}(\theta)\ \mathbb{Q}]$: divide a 2^{m+1}. Hemos demostrado la siguiente afirmación importante.

Si el campo numérico constructivo P es una ampliación algebraica final del campo $\mathbb{Q}$, entonces $[P : \mathbb{Q}] = 2^n$, para un cierto número entero no negativo n.

Este resultado permite responder a algunas cuestiones, planteadas incluso por los matemáticos de la antigüedad.

a) ¿Se puede construir (con ayuda de regla y compás) la arista de un cubo cuyo volumen es igual a 2 (problema hindú sobre la duplicación del cubo)? Se supone que nos es dado el cubo de volumen unitario. El polinomio $x^3 - 2$, cuya raíz es la magnitud de la arista buscada, es irreducible sobre $\mathbb{Q}$, puesto que $[\mathbb{Q}(\sqrt[3]{2})\ \mathbb{Q}] = 3 \neq 2^n$. El problema planteado tiene respuesta negativa.

b) ¿Cualquier ángulo puede ser dividido, con ayuda de la regla y el compás, en tres partes iguales (problema sobre la trisección del ángulo)? La respuesta es negativa, incluso para el ángulo concreto de 60°, por cuanto la constructividad de $\varphi = 20°$ significaría la constructividad de $\cos\varphi$ y de $2\cos\varphi$, y esto no es así. En efecto, según el teorema de Moivre, $1/2 = \cos 60° = \cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$, de modo que $\theta = 2\cos\varphi$ es la raíz del polinomio $f(x) = x^3 - 3x - 1 \in \mathbb{Z}[X]$. Puesto que ± 1 no son raíces de $f(x)$, entonces el polinomio $f(x)$ es irreducible sobre $\mathbb{Q}$ (véase el ejercicio 8, § 4, cap.6) y, en consecuencia, $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3 \neq 2^n$.

c) Razonamientos análogos muestran que el compás y la regla son insuficientes para la construcción de un polígono regular de n lados, para cualquier n natural. Por ejemplo, para $n = 7$ no es difícil convencerse de que la magnitud que debe ser construída $\theta =$

$= 2\cos\frac{360^\circ}{7}$ es una raíz irreducible sobre $\mathbb{Q}$ del polinomio x^3+x^2- $-2x-1$.

El genial Gauss, en el comienzo de su actividad como matemático, halló las condiciones necesarias y suficientes para n, con las cuales la construcción de un polígono regular de n lados es posible. El descubrió, en particular, que el número primo n debe ser un número de Fermat: $n = 2^{2^k} + 1$. La resolución completa de estas cuestiones se halla vinculada a las investigaciones del grupo de Galois del campo circular (véase el ejemplo 2).

EJERCICIOS

1. Mostrar, que la ampliación $F \supset P$ de grado simple, no tiene subcampo propios ($\neq P, F$).

2. Hallar el elemento primitivo de la ampliación $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, donde p y q son números primos.

3. Hallar la dimensión sobre $\mathbb{Q}$ del campo de descomposición del polinomio $X^p - 2$.

4. Mostrar, que sobre el campo P de característica $p > 0$ para el polinomio $X^p - a$, se tienen sólo dos posibilidades: ser irreducible, o ser polinomio lineal de grado p. (*Indicación.* Examinar el campo de descomposición F del polinomio $X^p - a$. Sea $\theta \in F$ una de las raíces, tal que $a = \theta^p$ y $X^p - a = (X - \theta)^p$. Si ahora $X^p - a = u(X)\, v(X)$, donde $u(X)$ es un polinomio unitario sobre P de grado positivo $m < p$, entonces, en virtud de la factoriabilidad de $F[X]$ se debe cumplir la igualdad $u(X) = (X - \theta)^m$. En particular, $\theta^m, \theta^p \in P \Rightarrow$ $\Rightarrow \theta \in P$.)

5. Sea $Z_p(Y)$, el campo de fracciones racionales de característica p. Mostrar, que $X^p - Y$ es un polinomio irreducible sobre $Z_p(Y)$, con todas sus raíces coincidentes. (*Indicación.* De acuerdo con el ejercicio anterior, es suficiente convencerse de que la igualdad $X^p - Y = \left(X - \frac{g(Y)}{h(Y)}\right)^p$ con $g, h \in Z_p[Y]$, es imposible.)

6. Demostrar que para cualquier $d \mid n$, $d < n$, tiene lugar la relación $X^n - 1 = (X^d - 1)\, \Phi_n(X)\, h_d(X)$, donde $h_d \in \mathbb{Z}[X]$. (*Indicación.* De acuerdo con (8), $X^d - 1 = \prod_{e \mid d} \Phi_e(X)$. Por eso

$$X^n - 1 = (X^d - 1) \prod_{s \mid n;\ s \nmid d} \Phi_s(X) = (X^d - 1)\, \Phi_n(X) \prod_{s \mid n;\ s \nmid d;\ s \neq n} \Phi_s(X).$$

Queda por referirse a (10).)

7. Sea q un número entero positivo >1. Conforme a (10), $\Phi_n(q) \in \mathbb{Z}$. Mostrar que $\Phi_n(q) \mid (q - 1) \Rightarrow n = 1$. (*Indicación.* Como $\Phi_n(X) = \prod (X - \varepsilon)$, donde ε recorre las raíces primitivas, entonces, cuando $n > 1$, todo $\varepsilon \neq 1$, y, por eso, la distancia, en el plano complejo, del punto q a cualquier ε es mayor que la distancia de q a 1. Por lo tanto, $|\Phi_n(q)| = \prod (q - \varepsilon) > q - 1$, y $q - 1$ de ningún modo es divisible por $\Phi_n(q)$.)

8. Comprobar, que el polinomio circular $\Phi_{15}(X) = X^8 - X^7 + X^5 -$ $- X^4 + X^3 - X + 1$, examinado sobre el campo $\mathbb{F}_2$, es el producto de dos polinomios irreducibles $X^4 + X^3 + 1$ y $X^4 + X + 1$. Aprovechando esta circunstancia demostrar la irreducibilidad de $\Phi_{15}(X)$ sobre $\mathbb{Q}$ (comparar con el ejercicio 11 § 1, cap. 6).

9. Partiendo de la cadena de inclusiones naturales

$$GF(p) \subset GF(p^{2!}) \subset GF(p^{3!}) \subset \ldots,$$

introducir el llamado *campo límite* $\Omega_p = GF(p^{\infty!})$, haciendo $\alpha \in \Omega_p \Leftrightarrow \{\alpha \in GF(p^{n!})$ para un n suficientemente grande$\}$. Apoyándose en las propiedades principales de los campos finitos, demostrar, que Ω_p es un campo algebraicamente cerrado. De este modo se obtienen, considerando el campo de los números complejos $\mathbb{C}$, ejemplos de campos algebraicamente cerrados, de cualquier característica.

10. Sea $q = p^n$. Mostrar, que cuando $p = 2$, todos los elementos del campo Γ_q son cuadrados, y para $p > 2$, los cuadrados del grupo Γ_q^* generan en el el subgrupo Γ_q^{*2} de índice 2, además, $\Gamma_q^{*2} = \operatorname{Ker}(t \mapsto t^{(q-1)/2})$.

11. (M. Aschbacher). *Sea Γ_q un campo finito con un número impar $q = p^n$ de elementos. Si $q \neq 3$ ó 5, entonces, en la circunferencia $x^2 + y^2 = 1$, existirá un punto con coordenadas x, $y \in \Gamma_q^*$.* Demostrar esta afirmación para $p > 5$. (*Indicación.* Pasar a la ecuación $x^2 + y^2 - z^2 = 0$, con $x, y, z \in \Gamma_p$. Según el teorema de Chevalier (véase el ejercicio 4, § 1, cap. 6) el número total N soluciones de esta ecuación se divide por p. Sea que no existen soluciones con $xyz = 0$. Calcular entonces N, considerando dos casos por separado. Si no existe $a \in \Gamma_p$ con $a^2 + 1 = 0$, entonces, sólo serán soluciones $(0, 0, 0)$, $(0, n, \pm n)$, $(n, 0, \pm n)$, $n = 1, 2, \ldots, p-1$, y, por eso, $N = 4p - 3 \equiv 0 \pmod{p} \Rightarrow p = 3$. Si $a^2 + 1 = 0$ para algún $a \in \Gamma_p$, entonces, $N = 6p - 5 \equiv 0 \pmod{p} \Rightarrow p = 5$).

12. ¿*Todo* elemento primitivo del campo Γ_q es generador del grupo multiplicativo Γ_q^*? (*Respuesta*: hablando en general, no.)

13. (*Teorema sobre el elemento primitivo.*) Sea $F = P(\theta_1, \theta_2, \ldots, \theta_r)$ una ampliación algebraica finita del campo P de característica nula. Mostrar, que $F = P(\theta)$ para cierto elemento algebraico θ sobre P. (*Indicación*. La inducción con respecto a r reduce el examen al caso de $F = P(\alpha, \beta)$, donde α y β son elementos algebraicos sobre P con distintos polinomios mínimos $f(X)$ y $g(X)$. Sea K el campo de descomposición del polinomio $f(X)\,g(X)$, tal que

$$f(X) = (X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n),\ \alpha_i \in K\ (\alpha_1 = \alpha)$$
$$g(X) = (X - \beta_1)(X - \beta_2)\ldots(X - \beta_m),\ \beta_j \in K\ (\beta_1 = \beta).$$

La irreducibilidad de $f(X)$ y de $g(X)$, así como la condición char $P = 0$, nos garantizan (véase el p. 4, § 1, cap. 6), que los elementos α_i, β_j difieren de par

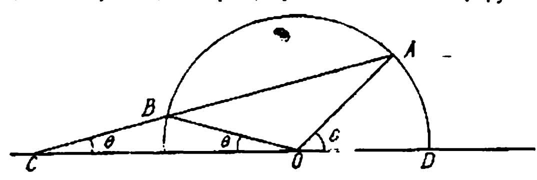


Fig. 23

en par, y que tenemos la posibilidad de construir los elementos $(\beta_j - \beta)/(\alpha - \alpha_i) \in K$, $i \neq 1$. Tomamos un número racional arbitrario $c \neq 0$, que difiera de estos elementos (¡nuevamente la condición char $P = 0$!) y hacemos

$$\theta = \beta + c\alpha.$$

Se comprende, que $P(\theta) \subset P(\alpha, \beta) = F$. Los polinomios $f(X)$ y $h(X) = g(\theta - cX) \in P(\theta)[X]$ tienen la raíz común α. Si α_i es también raíz común de los mismos en K, para cierto $i > 1$, entonces $0 = h(\alpha_i) = g(\theta - c\alpha_i)$, de donde $\theta - c\alpha_i = \beta_j$, para cierto $j \geqslant 1$. Pero esto significa, que bien

$c(\alpha - \alpha_j) = 0$, o que bien $c = (\beta_j - \beta)/(\alpha - \alpha_j)$. Ambas posibilidades se descartan en virtud de la elección de c y, por lo tanto, $X - \alpha$ es el máximo común divisor de los polinomios $f, h \in K[X]$. Pero, de hecho, $f, h \in P(\theta)[X]$, y por eso (véase el p. 3, § 3, cap. 5) m.c.d. $(f, h) \subset P(\theta)[X]$. Por lo visto, $X - \alpha \in P(\theta)[X]$, es decir, $\alpha \in P(\theta)$ y $\beta = \theta - c\alpha \in K(\theta)$. En este caso, $P(\alpha, \beta)$ $P(\ )$ y, por consiguiente, $P(\ ,\ ) = P(\ )$.

14. El dibujo (fig. 23) ilustra uno de los métodos de trisección de un ángulo: $\theta = \varphi/3$. Los segmentos OB y CB tienen una longitud igual a 1. ¿Cómo construir el punto A si el punto C está dado?

15. Mediante la formulación del campo numérico constructivo concreto P mostrar, que el grado de $[CS : \mathbb{Q}]$ es infinito.

§ 2. RESULTADOS PARCIALES SOBRE ANILLOS

Este parágrafo puede considerarse un pequeño pero útil complemento de los capítulos 4 y 5.

1. Nuevos ejemplos de anillos factoriales. En el § 3, cap. 5, fue demostrada la factoriabilidad de los anillos euclídeos, a los ejemplos conocidos de los cuales se refieren los anillos $\mathbb{Z}$ y $P[X]$. Más abajo se brinda otro ejemplo más de anillo euclídeo, así como de anillo factorial no euclídeo.

EJEMPLO 1 (*anillo de los números gaussianos enteros*). Se tiene en cuenta el anillo numérico

$$\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}\},$$

contenido en el campo cuadrático $\mathbb{Q}(i) \subset \mathbb{C}$, $i^2 + 1 = 0$, y geométricamente identificable con el conjunto de nudos (puntos) de una rejilla numérica entera en el plano complejo C. Es claro, que $\mathbb{Z}[i]$ es un anillo entero. Definemos en $\mathbb{Z}[i]^* = \mathbb{Z}[i] \setminus \{0\}$ la aplicación δ: $\mathbb{Z}[i]^* \to \mathbb{N} \cup \{0\}$, suponiendo $\delta(m + in) = |m + in|^2 = m^2 + n^2$ (en otras palabras, $\delta(a) = N(a)$ es la norma del número a en $\mathbb{Q}(i)$; véase el punto 5, § 1, cap. 5). Como se sabe, $\delta(ab) = \delta(a)\,\delta(b) \geqslant \delta(a)$ para todo $a, b \in \mathbb{Z}[i]^*$, así que la propiedad (E1) de la definición de anillo euclídeo (véase el punto 3, § 3, cap. 5) se cumple automáticamente. A fin de convencerse de la veracidad de (E2), escribamos la fracción ab^{-1} con $b \neq 0$, en la forma $ab^{-1} = \alpha + i\beta$, con $\alpha, \beta \in \mathbb{Q}$ y tomemos los números enteros k, l, más cercanos a α, β tales, que $\alpha = k + \nu$, $\beta = l + \mu$, $|\nu| \leqslant \frac{1}{2}$, $|\mu| \leqslant \frac{1}{2}$. Entonces

$$a = b\,[(k + \nu) + i\,(l + \mu)] = bq + r,$$

donde $q = k + ib \in \mathbb{Z}[i]$, y $r = b(\nu + i\mu)$. Como $r = a - bq$, también $r \in \mathbb{Z}[i]$, además

$$\delta(r) = |r|^2 = |b|^2(\nu^2 + \mu^2) \leqslant \delta(b)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{2}\,\delta(b) < \delta(b).$$

Por lo tanto, $\mathbb{Z}[i]$ es un *anillo euclídeo*. ∎

El anillo de los números enteros de Gauss $\mathbb{Z}[i]$ es cómodo para la demostración, en miniatura, de los métodos de la teoría de los nú-

meros algebraicos. Por eso, nos detendremos en las propiedades de $\mathbb{Z}[i]$ un poco más detalladamente. Al principio, hagamos algunas observaciones generales.

1) El anillo íntegro K, cuyos ideales son todos principales, o sea, tienen la forma xK, se llama *anillo de ideales principales. Todo anillo euclídeo es un anillo de ideales principales.* Para $\mathbb{Z}$ y $P[X]$, esto fue establecido antes (véase el corolario del teorema 5, § 2, cap. 5), y para el caso general la demostración es totalmente análoga si J es un ideal del anillo euclídeo K, entonces, $J = aK$, en cuanto $a \in J$ y $\delta(a) \leqslant \delta(x)$ para todo $0 \neq x \in J$. ∎

2) *Sean, K un anillo euclídeo arbitrario con función* δ (véase el punto 3, § 3, cap. 5) y $U(K)$ *el grupo de sus elementos reducibles. Entonces,*

$$u \in U(K) \Leftrightarrow \delta(u) = \delta(1) \Leftrightarrow \delta(ux) = \delta(x),\ \forall x \in K^*. \quad (1)$$

Efectivamente, de acuerdo con (E1), $\delta(x) = \delta(1 \cdot x) \geqslant \delta(1)$ para todo $x \in K^*$, y, si $u \in U(K)$, entonces, $\delta(1) = \delta(u \cdot u^{-1}) \geqslant \delta(u)$, así que $\delta(u) = \delta(1)$. Recíprocamente, en correspondencia con la observación 1), $\delta(ux) = \delta(x)$, $\forall x \in K^* \Rightarrow uxK = xK \Rightarrow x = uxv \Rightarrow uv = 1 \Rightarrow u \in U(K)$.

El empleo del criterio (1) con respecto al anillo $\mathbb{Z}[i]$ significa que $m + in \in U(\mathbb{Z}[i]) \Leftrightarrow m^2 + n^2 = 1$. *Por lo tanto,* $U(\mathbb{Z}[i]) = \langle i \rangle$, *es un grupo cíclico de orden* 4.

3) El ideal J del anillo K se llama *máximo*, si $J \neq K$ y todo ideal T, contenedor de J, coincide con K o J. *En el anillo euclídeo K la propiedad del elemento $p \in K$ de ser primo, es equivalente a la condición de que el ideal pK sea máximo.*

En efecto, sean, p un elemento primo, y $pK \subset T \subset K$, donde T es un ideal en K. De acuerdo con 1) $T = aK$, y, como $p \in T$, entonces, $p = ab$, donde uno de los elementos a, b, es invertible. Si $a \in U(K)$, entonces, $T = aK = K$. Si $b \in U(K)$, entonces, $T = aK = abK = pK$. Recíprocamente, sea el ideal pK máximo y $p = ab$, con $a \notin U(K)$. En este caso $aK \neq K$ y $pK \subset aK \Rightarrow pK = aK \Rightarrow a = pu = abu \Rightarrow bu = 1 \Rightarrow b \in U(K) \Rightarrow p$ es un elemento primo.

Veamos ahora que pasa con el número primo $p \in \mathbb{Z}$ en el anillo $\mathbb{Z}[i]$. No se exluye, que p quede como elemento primo en $\mathbb{Z}[i]$, pero si esto no es así, entonces, sea $p = \prod_{k=1}^{r} p_k$ su descomposición única (según el teorema 4, § 3, cap. 5) en r factores primos p_k $(r > 1)$. Conforme a 2), $\delta(p_k) > 1$, así que, de $p^2 = \delta(p) = \Pi\delta(p_k)$ y de la factoriabilidad de $\mathbb{Z}$ se deducen, necesariamente, las igualdades $r = 2$, $p = p_1p_2$, $\delta(p_1) = \delta(p_2) = p$. Si $p_1 = m + in$, entonces, $p = \delta(p_1) = m^2 + n^2 = (m + in)(m - in) \Rightarrow p_2 = m - in$. Y bien, *si el número primo $p \in \mathbb{Z}$ permite una descomposición no trivial en*

$\mathbb{Z}[i]$, *entonces*

$$p = (m + in)(m - in) = m^2 + n^2, \qquad (2)$$

donde $m + in$, $m - in$, *son elementos primos en* $\mathbb{Z}[i]$. ∎

En particular, $2 = (1 + i)(1 - i)$ no es elemento primo en $\mathbb{Z}[i]$. Observemos, más adelante, que $t^2 \equiv 0$ ó $1 \pmod 4$ para cualquier $t \in \mathbb{Z}$. Por eso, para un número primo impar p, que no es primo en $\mathbb{Z}[i]$, el criterio (2) lleva a la conclusión:

$$p = m^2 + n^2 \equiv 0,\ 1 \text{ ó } 2 \pmod 4) \Rightarrow p = 4k + 1.$$

Cuando $p = 4k + 1$, hagamos $t = (2k)!$. Como, evidentemente, $t = (-1)^{2k}(2k)! = (-1)(-2)\ldots(-2k) \equiv (p - 1) \times \times (p - 2) \ldots (p - 2k) \equiv ((p + 1)/2) \ldots (p - 2)(p - 1) \times \times \pmod p$, entonces

$$t^2 \equiv (2k)!\,((p + 1)/2) \ldots (p - 2)(p - 1) \equiv (p - 1)! \pmod p,$$

o, teniendo en cuenta el teorema de Wilson (véase el final del § 1, cap. 6), $t^2 + 1 \equiv 0 \pmod p$. Si ahora p es un elemento primo en $\mathbb{Z}[i]$, entonces, de la igualdad $(t + i)(t - i) = t^2 + 1 = lp$, $l \in \mathbb{Z}$, según el teorema 1, § 3, cap. 5, se deduce la divisibilidad por p de uno de los elementos $t + i$, $t - i$. Pero, $t \pm i = p(m + in) \Rightarrow \pm 1 = pn$, $n \in \mathbb{Z}$, lo que es claramente imposible. Hemos demostrado la afirmación siguiente.

El número primo $p \in \mathbb{Z}$ *queda como primo en* $\mathbb{Z}[i]$, *si, y sólo si,* $p = 4k - 1$.

Cualquier número primo $p = 4k + 1$ *es expresable en la forma* $p = m^2 + n^2$, *donde* $m, n \in \mathbb{Z}$. ∎

De aquí, con relativa facilidad, se extrae el teorema teórico-numérico general.

TEOREMA 1. *El número* $t \in \mathbb{Z}$ *es expresable en forma de suma de cuadrados de dos números* $m, n \in \mathbb{Z}$ *si, y sólo si, en la descomposición canónica de* t *en sus factores primos, cada divisor primo* $p = 4k - 1$ *figura con exponente par.*

En efecto, como agregado a los hechos que conocemos, es suficiente mostrar, que *si* el m.c.d. $(m, n) = 1$ *y* $p \mid (m^2 + n^2)$, *entonces*, $p = 4k + 1$. Esto es suficientemente claro: m.c.d. $(m, n) = 1$, $m^2 + n^2 \equiv 0 \pmod p \Rightarrow mn \not\equiv 0 \pmod p \Rightarrow m^{p-1} \equiv 1 \pmod p$, $n^2 \equiv -m^2 \pmod p \Rightarrow (m^{p-2}n)^2 = m^{2p-4}n^2 \equiv -m^{2p-2} \equiv -1 \pmod p$. De este modo, existe un número entero $s \in \mathbb{Z}$ tal, que $s^2 \equiv -1 \pmod p$, $s^4 \equiv 1 \pmod p$. Por lo tanto, el grupo multiplicativo Z_p^* de orden $p - 1$ se divide por 4 y $p = 4k + 1$. ∎

De acuerdo con la observación 3), que $p = 4k - 1$ sea primo en $\mathbb{Z}[i]$ es equivalente a que sea máximo el ideal $p\mathbb{Z}[i]$, lo que, a su vez, se expresa mediante la propiedad del anillo cociente $\mathbb{Z}[i]/p\mathbb{Z}[i]$ de ser un campo de p^2 elementos (véase, en relación con esto, el ejercicio 14, § 4, cap. 4, y los teoremas sobre el isomorfismo para los anillos en el punto 2). Esto no es sorprendente, si se toma en

consideración, que cuando $p = 4k - 1$, el polinomio $X^2 + 1$, examinado sobre Z_p, es irreducible.

EJEMPLO 2 (*ampliaciones polinómicas de anillos factoriales*). Ahora se mostrará, que los anillos de los polinomios $Z[X_1, \ldots, X_n]$ y $P[X_1, \ldots, X_n]$ (P es un campo) son factoriales para cualquier n. Esta importante afirmación, surge inmediatamente del teorema siguiente.

TEOREMA 2. *Si el anillo K es factorial, también lo será el anillo de los polinomios $K[X]$.*

DEMOSTRACION La demostración se basa en las propiedades de los anillos de los polinomios, adjuntas al lema de Gauss (véase § 3, cap. 5). Precisamente, nos son necesarias las dos propiedades siguientes.

a) *Los polinomios primitivos $f, g \in K[X]$, asociados en $Q(K)[X]$* ($Q(K)$, que es el campo de relaciones del anillo factorial K), *son asociados en $K[X]$* (un ejercicio fácil).

b) *El polinomio $f \in K[X]$ de grado positivo, irreducible sobre K, también es irreducible sobre $Q(K)$* (la demostración en el § 3, cap. 5 para $K = Z$, sirve para el caso general).

Pasando inmediatamente a la demostración del teorema, escribamos el polinomio $f \in K[X]$ de grado positivo, en la forma $f = d(f) f_0$, donde $d(f)$ es el contenido de f, y f_0 es el polinomio primitivo. Por inducción con respecto al grado de los polinomios primitivos, obtenemos la descomposición de f_0 en el producto $f_0 = f_1 \ldots f_s$ de los polinomios primitivos $f_1, \ldots, f_s$ irreducibles sobre K. Sea $f_0 = g_1 \ldots g_t$ otra descomposición semejante más. Entonces, de acuerdo con b), f_i y g_j son irreducibles sobre $Q(K)$, y, por cuanto el anillo $Q(K)[X]$ es factorial (corolario del teorema 4, § 3, cap. 5), $s = t$, y, para un ordenamiento debido del polinomio f_i asociado con g_i en $Q(K)[X]$, y, por consiguiente (según *a*)), en $K[X]$. En lo que respecto al polinomio f con contenido $d(f)$ irreducible en K, entonces, tomando también la descomposición de $d(f) = p_1 \ldots p_2$ en factores primos $p_i \in K$, llegaremos a la descomposición de f. La unicidad de tal descomposición (en su concepción habitual) se deduce de la recientemente establecida unicidad de la descomposición f_0 y de la factorizabilidad de K, que responde a la unicidad de la descomposición $d(f) = p_1 \ldots p_r$. ∎

Tienen lugar las inclusiones rigurosas

$$\left\{\begin{array}{c}\textit{anillos}\\ \textit{euclídeos}\end{array}\right\} \subset \left\{\begin{array}{c}\textit{anillos de idea-}\\ \textit{les principales}\end{array}\right\} \subset \left\{\begin{array}{c}\textit{anillos}\\ \textit{factoriales}\end{array}\right\} \qquad (3)$$

La primera inclusión nos es conocida (véase la observación (1)). Existen ejemplos (que no ponemos), que indican su rigurosidad. Para demostrar la segunda inclusión, examinemos en el anillo de ideales principales K, la sucesión creciente de ideales $(d_1) \subset (d_2) \subset \ldots$

Se comprueba inmediatamente, que $D = \bigcup_i (d_i)$ es un ideal en K. Por consiguiente, $D = (d)$, $d \in D$. Por definición, $d \in (d_m)$ para cierto m, de donde, $(d_m) = (d_{m+1}) = \ldots$ La estabilización, en el paso final de la cadena creciente de ideales conlleva la ruptura de la cadena de divisores no invertibles $d_1, d_2, d_3, \ldots$ con $d_i \mid d_{i-1}$ y, por lo tanto, la existencia de la descomposición en K en elementos indescomponibles. La unicidad de la descomposición en K es consecuencia de las mismas causas $(a, b) \Rightarrow aK + bK = dK = (d) \Rightarrow$ $\Rightarrow d = \text{m.c.d.}\ (a, b) = ax + by$. Los razonamientos posteriores repiten la demostración del teorema 3 (ii), § 3, cap. 5.

Los ideales $(2, X)$ en $\mathbb{Z}[X]$ y (X, Y) en $\mathbb{R}[X, Y]$ no son principales (véase el ejemplo en el punto 3, § 2, cap. 5). Al mismo tiempo, de acuerdo con el teorema 2, los anillos $\mathbb{Z}[X]$ y $\mathbb{R}[X, Y]$ son factoriales. Con esto, la veracidad de la cadena (3) queda establecida.

Los anillos de ideales principales, son interesantes desde un punto de vista puramente algebraico, por cuanto ellos se caracterizan por las propiedades de tales objetos naturales, como los núcleos de homomorfismos. Por otra parte, los anillos euclídeos son más cómodos para la investigación, en virtud de que en ellos se encuentra el algoritmo de división con resto.

2. **Estructuras teórico-anulares.** Ya disponemos de un arsenal considerable de tipos de anillos y de medios que permiten construir nuevos anillos, a partir de un cúmulo dado de ellos. Sirven de ejemplos, las estructuras del anillo de las matrices $M_n(K)$, del campo de relaciones $Q(K)$ y del anillo de los polinomios $K[X_1, \ldots, X_n]$, donde K es un anillo conmutativo (entero, cuando $Q(K)$). Es útil considerar también, aunque sea brevemente, los análogos teórico-anulares de los hechos comunes sobre los homomorfismos, que fueron establecidos para los grupos en el cap. 7. Las demostraciones, por regla, no se diferencian en nada del caso de los grupos, y se dejan al lector en calidad de ejercicios.

Al teorema fundamental sobre los homomorfismos para los anillos (teorema 2, § 4, cap. 4), lo complementaremos con dos teoremas sobre el isomorfismo.

TEOREMA 3. *Sean, K un anillo; L un subanillo; J un ideal en K. Entonces, $L + J = \{x + y \mid x \in L,\ y \in J\}$ es un subanillo en K, contenedor de J en calidad de ideal, $L \cap J$ es un ideal en L. La aplicación*

$$\varphi: x + J \mapsto x + L \cap J, \quad x \in L,$$

realiza el isomorfismo de los anillos:

$$(L + J)/J \cong L/L \cap J.$$

DEMOSTRACIÓN. Las dos primeras afirmaciones son totalmente evidentes. En lo que respecta a la última, es necesario examinar la limi-

tación $\pi_0 = \pi \mid_L$ del epimorfismo natural $\pi: K \to K/L$. Su imagen $\operatorname{Im} \pi_0$ se compone de las clases adjuntas $x + J$, $x \in L$, o sea, $\operatorname{Im} \pi_0 = (L + J)/J$. El núcleo $\operatorname{Ker} \pi_0$ del epimorfismo $\pi_0: L \to \to (L + J)/J$ está integrado por los elementos $x \in L$, para los cuales $x + J = J$. En consecuencia, $\operatorname{Ker} \pi_0 = L \cap J$. Según el teorema fundamental sobre los homomorfismos, la correspondencia $\bar{\pi}_0 : x + + L \cap J \to \pi_0(x) = x + J$ establece el isomorfismo $L/L \cap J \cong \cong (L + J)/J$. Queda por observar, que $\varphi = \bar{\pi}_0^{-1}$. ∎

Hemos efectuado este razonamiento, copiado de la demostración del teorema 2, § 3, cap. 7, a fin de subrayar el paralelismo total con la teoría de grupos.

TEOREMA 4. *Sean, K un anillo; J, L subanillos del mismo, además, J es un ideal en K y $J \subset L$. Entonces, $\bar{L} = L/J$ es un subanillo en K/J y $\pi^*: L \to \bar{L}$ es una aplicación biyectiva del conjunto $\Omega(K, J)$ de los subanillos en K*, contenedores de J, en el conjunto $\Omega(\bar{K})$ de todos los subanillos del anillo $\bar{K}$. *Si $L \in \Omega(K, J)$, entonces, L es un ideal en K si, y sólo si, $\bar{L}$ es un ideal en $\bar{K}$, además*

$$K/L \cong \bar{K}/\bar{L} = (K/J)/(L/J).$$

DEMOSTRACION. Este es un ejercicio sencillo (véase la demostración del teorema 3, § 3, cap. 7). ∎

COROLARIO. *Sea K un anillo conmutativo con unidad 1. El ideal J es máximo en K si, y sólo si, el anillo cociente K/J es un campo.*

En el conjunto de ideales del anillo K están definidas las operaciones siguientes

suma: $J_1 + J_2 = \{x_1 + x_2 \mid x_k \in J_k\}$,
intersección: $J_1 \cap J_2 = \{x \mid x \in J_1,\ x \in J_2\}$,
producto: $J_1 J_2 = \{\sum_i x_{1i} x_{2i} \mid x_{ki} \in J_k\} \subset J_1 \cap J_2$.

También se puede hablar sobre la suma, intersección y producto de cualquier número finito de ideales, siendo legítima la afirmación siguiente.

PROPOSICION. *Si en el anillo K con unidad, tienen lugar las igualdades*

$$J + J_k = K, \quad k = 1, \ldots, n,$$

para los ideales J, $J_1, \ldots, J_n$, entonces, también son correctas las igualdades

$$J + J_1 \cap J_2 \cap \ldots \cap J_n = K = J + J_1 J_2 \ldots J_n.$$

DEMOSTRACION. Como $J_1 J_2 \ldots J_n \subset J_1 \cap J_2 \cap \ldots \cap J_n$, en consecuencia, es suficiente establecer la igualdad $J + J_1 J_2 \ldots J_n = = K$. Para $n = 1$, ella es exacta por condición. Para $n = 2$, te-

nemos

$$1 = 1^2 = (x_1 + y_1)(x_2 + y_2) = x + y_1 y_2,$$

donde $x_1, x_2 x \in J$, $y_i \in J_i$. Por lo tanto, $1 \in J + J_1 J_2$ y $K = J + J_1 J_2$. Luego es evidente la inducción con respecto al número n. ∎

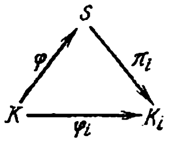
Sean, $K_1, \ldots, K_n$, una familia finita de anillos, $K = K_1 \times \ldots \times K_n$, el producto cartesiano de los conjuntos. Introduzcamos en K la estructura de anillo, definiendo la operación de suma y multiplicación por componentes:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n);$$
$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$

Llegamos a la *suma directa exterior* $K = K_1 \oplus \ldots \oplus K_n$ de los *anillos* K_i. Cada uno de los componentes de K_i es una imagen para el epimorfismo π_i: $K \to K_i$, π_i: $(x_1, \ldots, x_n) \mapsto x_i$, $1 \leqslant i \leqslant n$. Si, luego, $J_i = \{(0, \ldots, x_i, \ldots, 0) \mid x_i \in K_i\}$, entonces, $J_i \cong K_i$, J_i es un ideal en K, y $K = J_1 + \ldots + J_n$.

Sea ahora K un anillo con ideales $J_1, \ldots, J_n$, además, $K = J_1 + \ldots + J_n$ y $J_k \cap (\sum_{j \neq k} J_j) = 0$, $1 \leqslant k \leqslant n$. En este caso, $K = J_1 \oplus \ldots \oplus J_n$, es la *suma directa interna* de sus *ideales* J_k. Al igual que en la teoría de los grupos, la diferencia entre las sumas directas internas y externas de los anillos es puramente teórica-de conjunto y no tiene sentido reflejarla en las designaciones.

3. Aplicaciones teórico-numéricas. La propiedad universal de las sumas directas, consiste en que, *si* $S = K_1 \oplus \ldots \oplus K_n$ y K *es un anillo cualquiera con los homomorfismos dados* φ_i: $K \to K_i$, *existirá un único homomorfismo* $\varphi = (\varphi_1, \ldots, \varphi_n)$: $K \to S$, *con núcleo* Ker $\varphi = \bigcap$ Ker φ_i, *que hace conmutativos los diagramas triangulares*



para $i = 1, \ldots, n$. Apliquemos esta afirmación evidente al anillo K con 1 y con ideales $J_1, \ldots, J_n$, y a la suma directa

$$S = K/J_1 \oplus \ldots \oplus K/J_n.$$

Haciendo φ_i: $K \to K/J_i = K_i$, obtendremos el homomorfismo

$$\varphi: x \mapsto (x + J_1, \ldots, x + J_n) \qquad (4)$$

del anillo K en S con núcleo Ker $\varphi = J_1 \cap \ldots \cap J_n$.

TEOREMA 5 (teorema chino sobre los restos). *Si en las condiciones indicad más arriba*, K es un anillo *con unidad y* $J_i + J_j = K$ para

$1 \leqslant i \neq j \leqslant n$, *entonces, la aplicación* φ (véase (4)) *es un epimorfismo.*

DEMOSTRACIÓN. Necesitamos convencernos de que para cualesquiera elementos $x_1, \ldots, x_n \in K$ dados, existirá un $x \in K$, para el cual $x_i + J_i = x + J_i$, o sea, $x - x_i \in J_i$, $i = 1, 2, \ldots, n$. Para $n = 1$ esto es evidente, y para $n = 2$ tomamos los elementos $a_1 \in J_1$, $a_2 \in J_2$, para los que $a_1 + a_2 = 1$, y hacemos $x = x_1a_2 + x_2a_1$. Entonces,

$$x - x_1 = (x_1a_2 + x_2a_1) - x_1(a_1 + a_2) = (x_2 - x_1)a_1 \in J_1,$$
$$x - x_2 = (x_1a_2 + x_2a_1) - x_2(a_1 + a_2) = (x_1 - x_2)a_2 \in J_2.$$

Luego, razonamos por inducción con respecto a n. Sea que ya hallamos el elemento y, para el cual $y - x_i \in J_i$, $i = 1, 2, \ldots, n - 1$. Como, por condición, $J_i + J_n = K$, $1 \leqslant i \leqslant n - 1$, entonces, de acuerdo con la proposición del punto 2, $J_1 \cap \ldots \cap J_{n-1} + J_n = K$. Aplicando el caso analizado $n = 2$ a los ideales $J_1 \cap \ldots \cap J_{n-1}$, J_n, y a los elementos $y, x_n \in K$, hallaremos $x \in K$, con $x - y \in J_1 \cap \ldots \cap J_{n-1}$, $x - x_n \in J_n$. Pero, $x - y \in J_1 \cap \ldots \cap J_{n-1} \Rightarrow x - y \in J_i$, $1 \leqslant i \leqslant n - 1$. Tomando en cuenta la elección de y, obtenemos

$$x - x_i = (x - y) + (y - x_i) \in J_i, \quad 1 \leqslant i \leqslant n - 1.$$

Por lo tanto, el elemento x satisface todas las condiciones requeridas. ∎

En el teorema 5 así como en todos los razonamientos que lo preceden, el anillo K no se suponía conmutativo. Sea, luego, K un anillo íntegro, y $a_1, \ldots, a_n$, sus n de elementos primos entre sí de dos en dos, o sea, $a_iK + a_jK = K$ para $i \neq j$ (en el anillo factorial K, esta definición concuerda con la de indivisibilidad, obtenida de la descomposición de a_i en sus factores primos). Escribiendo la inclusión $x - x_i \in a_iK$ en forma de comparación con respecto al módulo del ideal principal a_iK, como de costumbre, utilizamos la notación $x \equiv x_i \pmod{a_i}$.

COROLARIO 1. *Sean, K, un anillo íntegro, y $a_1, \ldots, a_n$, sus elementos primos entre sí de dos en dos. Entonces, para cualesquiera $x_1, \ldots, x_n \in K$, existirá un elemento $x \in K$ tal, que* $x \equiv x_i \pmod{a_i}$, *$i = 1, \ldots, n$.* ∎

COROLARIO 2. *Sea n un número natural, con la descomposición canónica $n = p_1^{m_1} \ldots p_r^{m_r}$, $Z_n = \mathbb{Z}/n\mathbb{Z}$, el anillo de la clase de restos respecto al módulo n, y $U(Z_n)$ el grupo multiplicativo de sus elementos invertibles. Entonces:*

(i) $Z_n \cong Z_{p_1^{m_1}} \oplus \ldots \oplus Z_{p_r^{m_r}}$ (*suma directa de anillos*);

(ii) $U(Z_n) \cong U(Z_{p_1^{m_1}}) \times \ldots \times U(Z_{p_r^{m_r}})$ (*producto directo de grupos*).

DEMOSTRACION. (i) Sustituyendo en (4) n por r, haciendo $K = \mathbb{Z}$, $J_i = p_i^{m_i}\mathbb{Z}$ y $S = Z_{p_1^{m_1}} \otimes \ldots \otimes Z_{p_r^{m_r}}$ llegaremos al homomorfismo $\varphi: \mathbb{Z} \to S$, con núcleo $\mathrm{Ker}\,\varphi = \bigcap J_i = n\mathbb{Z}$. Que φ sea epimorfo se deduce del teorema 5, por cuanto el m.c.d. $(p_i, p_j) = 1$, para $i \neq j$.

(ii) Como en la suma directa arbitraria $K = K_1 \oplus \ldots \oplus K_r$ los componentes K_i se anulan entre sí: $K_iK_j = 0$, $i \neq j$, entonces, inmediatamente de la definición de elementos invertibles se deriva que $U(K) = U(K_1) \times \ldots \times U(K_r)$. Queda por aplicar esto a la descomposición (i). ■

OBSERVACION. De la afirmación (ii) se aprecia inmediatamente que $\varphi(n) = \prod_{i=1}^{r} \varphi(p^{m_i})$, y, como $\varphi(p^m) = p^{m-1}(p-1)$, se obtiene de nuevo la fórmula para los valores de la función de Euler (véase el ejemplo 1, punto 4, § 1). El orden de un elemento de un grupo finito, es divisor del orden del grupo, por eso

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

para cualquier número entero a, primo entre sí con n (generalización del pequeño teorema de Fermat, conocido bajo el nombre de teorema de Euler).

A fin de comprender definitivamente la estructura del grupo $U(Z_n)$, en virtud del corolario 2, nos es suficiente aclarar el caso $n = p^m$.

TEOREMA 6. *Sea m un número entero positivo.*

(i) *Si p es un número primo impar, entonces, $U(Z_{p^m})$ es un grupo cíclico.*

(ii) *Los grupos $U(Z_2)$ y $U(Z_4)$ son cíclicos de orden 1 y 2, respectivamente, al mismo tiempo que $U(Z_{2^m})$, $m \geqslant 3$, es el producto directo de un grupo cíclico de orden 2^{m-2} por un grupo cíclico de orden 2.*

DEMOSTRACION. (i) Por definición, el número entero t, primo entre sí con n, tiene el *orden r con respecto al módulo n*, si $| \langle t + n\mathbb{Z} \rangle | = r$, o sea, $t^r \equiv 1 \pmod{n}$, $t^k \not\equiv 1 \pmod{n}$ para $k < r$. Cuando $r = \varphi(n)$ se habla sobre la *raíz primitiva* (o *prototipo*) t *respecto al módulo n*. Habitualmente t se toma de un sistema de restos $0, 1, \ldots, n-1$ respecto al módulo n, expuesto, pero nosotros no fijamos ningún sistema de restos.

De acuerdo con el teorema 5, § 1, el grupo $Z_p^* = U(Z_p)$ es cíclica, o sea, existe la raíz primitiva a_0 respecto al módulo p. Como $a_0^{p^{m-1}} \equiv a_0 \pmod{p}$, entonces, también el número entero $a = a_0^{p^{m-1}}$ será raíz primitiva respecto al módulo p. Por otra parte, $a^{p-1} = a_0^{p^{m-1}(p-1)} = a_0^{\varphi(p^m)} \equiv 1 \pmod{p^m}$. En consecuencia, la clase adjunta $\bar{a} = a + p^m\mathbb{Z}$ engendra en $U(Z_{p^m})$ un subgrupo cíclico de orden $p-1$.

Luego,

$$(1+p)^p = \sum_{i=0}^{p} \binom{p}{i} p^i = 1 + p^2 + \frac{1}{2}(p-1)p^3 + \sum_{i\geq 3} \binom{p}{i} p^i.$$

Como $p > 2$, entonces, $(1+p)^p \equiv 1 + p^2 \pmod{p^3}$. Presuponiendo por inducción, que $(1+p)^{p^j} \equiv 1 + p^{j+1} \pmod{p^{j+2}}$, hallamos

$$(1+p)^{p^{j+1}} = [1 + (1+sp)\, p^{j+1}]^p = \sum_{i=0}^{p} \binom{p}{i} (1+sp)^i p^{(j+1)i} =$$

$$= 1 + (1+sp)\, p^{j+2} + \frac{1}{2}(p-1)(1+sp)^2 p^{2(j+1)+1} + \ldots$$

de donde, $(1+p)^{p^{j+1}} \equiv 1 + p^{j+2} \pmod{p^{j+3}}$. En particular, $(1+p)^{p^{m-1}} \equiv 1 \pmod{p^m}$, pero, $(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \not\equiv 1 \pmod{p^m}$ y, por lo tanto, la clase adjunta $\bar{b} = 1 + p + p^m Z$ con representante $b = 1 + p$, engendra en $U(Z_{p^m})$ un grupo cíclico de orden p^{m-1}. De acuerdo con la proposición del punto 3, § 2, cap 4, los elementos $\bar{a}$, $\bar{b}$ primos entre sí de órdenes $p - 1$, p^{m-1}, engendran el grupo cíclico $\langle \bar{a}\bar{b} \rangle$ de orden $p^{m-1}(p-1) = \varphi(p^m) = |U(Z_{p^m})|$.

(ii) Con los grupos $U(Z_2)$ y $U(Z_4)$ está todo claro. Cuando $m > 2$, partiendo de la comparación trivial $5 \equiv 1 + 2^2 \pmod{2^3}$, por inducción con respecto a j, se comprueba fácilmente, que

$$5^{2^j} \equiv 1 + 2^{j+2} \pmod{2^{j+3}}.$$

En particular,

$$5^{2^{m-3}} \equiv 1 + 2^{m-1} \not\equiv 1 \pmod{2^m}, \quad 5^{2^{m-2}} \equiv 1 \pmod{2^m},$$

así que 5 tiene orden 2^{m-2} respecto al módulo 2^m y la clase adjunta $5 + 2^m\mathbb{Z}$ engendra en $U(Z_{2^m})$ un subgrupo cíclico de índice 2. Observemos, que $-1 + 2^m\mathbb{Z} \notin \langle 5 + 2^m\mathbb{Z} \rangle$, por cuanto $5^j \equiv -1 \pmod{2^m} \Rightarrow 5^j \equiv -1 \pmod 4 \Rightarrow 1 \equiv -1 \pmod 4$, es una contradicción. Como $|\langle -1 + 2^m\mathbb{Z} \rangle| = 2$, entonces,

$$U(\mathbb{Z}/2^m\mathbb{Z}) = \langle 5 + 2^m\mathbb{Z} \rangle \times \langle -1 + 2^m\mathbb{Z} \rangle$$

es un 2-grupo abeliano del tipo $(2^{m-2}, 2)$ (véase el § 5, cap. 7). ∎

COROLARIO. *El grupo $U(Z_n)$ es cíclico (o, lo que es equivalente, existe la raíz primitiva respecto al módulo n si, y sólo si, el número entero $n > 1$ tiene la forma* 2, 4, p^m *o* $2p^m$, donde p es un número primo impar.

EJERCICIOS

1. Demostrar, que el elemento no nulo p del anillo factorial K resulta primo si, y sólo si, K/pK es un anillo íntegro.
2. Demostrar, que si el anillo íntegro K no es un campo, entonces, $K[X]$ no es anillo de los ideales principales.

3. Mostrar, que los elementos $x+y\sqrt{-3}$ con $x, y \in \mathbb{Z}$, o $x=\frac{2k+1}{2}$, $y=\frac{2l+1}{2}$, $k, l \in \mathbb{Z}$, componen el anillo íntegro K. Comprobar, que él es euclídeo con función $\delta = N$ (norma en $\mathbb{Q}(\sqrt{-3})$). Mostrar, que el subanillo $\mathbb{Z}[\sqrt{-3}] \subset K$ no es siquiera factorial.

4. Hallar todos los elementos primos del anillo de los números enteros de Gauss.

5. Perfeccionar el corolario del teorema 5 en el caso del anillo factorial K, para lo cual, junto con los elementos primos entre sí de dos en dos $a_1, \ldots, a_n$, introducir los elementos $\tilde{a}_i = \prod_{j \neq i} a_j$. Hallar los $b_i \in K$, para los cuales $b_i \equiv 1 \pmod{a_i}$, $b_i \equiv 0 \pmod{\tilde{a}_i}$, $1 \leqslant i \leqslant n$. Sean $x_1, \ldots, x_n \in K$. Introducir el elemento $x = \sum b_i x_i$ y comprobar, que $x \equiv x_i \pmod{a_i}$, $1 \leqslant i \leqslant n$ (una comodidad, apreciable en aquellos casos, cuando se trata de un número grande de colecciones $x_1, \ldots, x_n$).

6. Aplicar el ejercicio anterior a los módulos $a_1 = 5$, $a_2 = 9$ y a los pares $(x_1, x_2) = (2,5), (3,2), (3,5)$. ¿Qué se puede decir sobre el orden x respecto al módulo 45?

7. Sea p un número primo impar. Si la comparación $x^2 \equiv a \pmod{p}$ tiene solución, entonces, el número entero a se llama *resto cuadrático respecto al módulo p*, en caso contrario, *no resto cuadrático*. El *símbolo de Legendre* $\left(\frac{a}{p}\right)$ se define por la relación

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{si } a \equiv 0 \pmod{p}, \\ 1, & \text{si } a \not\equiv 0 \pmod{p}, \text{ es resto cuadrático}, \\ -1, & \text{si } a \not\equiv 0 \pmod{p}, \text{ es no resto cuadrático}. \end{cases}$$

Mostrar, pue $\left(\frac{a}{p}\right) = 1 \Longleftrightarrow a + pZ \in \mathbb{Z}_p^{*2}$ y $\left(\frac{a}{p}\right) \equiv a \qquad (\text{mod } p)$.

Luego, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ y el número de restos cuadráticos en el sistema reducido $1, 2, \ldots, p-1$, coincide con el número de no restos. Comprobar, para los pequeños números primos impares p y q, el cumplimiento de la *ley cuadrática de reciprocidad*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

demostrado en general (de muchas maneras) por Gauss. Extraer del ejemplo 1 en el punto 1, la relación $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

8. Demostrar (en términos del ejercicio anterior), que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, o sea, 2 resulta cuadrado respecto al módlou p exactamente entonces, cuando $p \equiv \pm 1 \pmod{8}$. (*Indicación*. Haciendo hincapié en el ejercicio 9, § 1, examinar la raíz primitiva α de potencia 8 de 1 en el cierre algebraico Ω_p del campo F_p. Como $\alpha^4 = -1$, entonces, $\alpha^2 + \alpha^{-2} = 0$; además, $\alpha^5 = -\alpha$, $\alpha^{-5} = -\alpha^{-1}$,

de donde, $\alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1})$. Haciendo $\beta = \alpha + \alpha^{-1}$, tendremos: $\beta^2 = \alpha^2 + \alpha^{-2} + 2 = 2$, así que $p \equiv \pm 1 \pmod 8 \Rightarrow \beta^p = \alpha^p + \alpha^{-p} = \alpha + \alpha^{-1} = \beta \Rightarrow 1 = \beta^{p-1} = (\beta^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \Rightarrow \left(\frac{2}{p}\right) = 1$. Análogamente, $p \equiv \pm 5 \pmod 8 \Rightarrow \beta^p = \alpha^p + \alpha^{-p} = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -\beta \Rightarrow -1 = \beta^{p-1} = 2^{\frac{p-1}{2}} \Rightarrow \left(\frac{2}{p}\right) = -1$.)

9 (complemento del punto 5, § 2, cap. 3). Sea $f(X) = f(\ldots, x_{ij}, \ldots)$ un polinomio no nulo con coeficientes en $\mathbb{Z}$ o en algún campo, de n^2 variables independientes $x_{ij} \in K$, $1 \leqslant i, j \leqslant n$, considerado como función de la matriz $X = (x_{ij})$. Demostrar, que si $f(XY) = f(X) f(Y)$ para todos los $X, Y \in M_n(K)$, entonces, $f(X) = (\det X)^m$, donde m es algún número entero no negativo. En particular, $f(X) = \det X$, si $f(\operatorname{diag}(x, 1, \ldots, 1)) = x$. (*Indicación*. Si $n = 1$ y $f(x) = \sum_{i=1}^{m} a_i x^i$, $a_m \neq 0$, entonces

$$f(xy) = \sum_{i=1}^{m} a_i x^i y^i = f(x) f(y) = f(x) \left(\sum_{i=1}^{m} a_i y^i\right)$$

donde x, y, son variables independientes. La igualdad de los coeficientes de y^m muestra, que $a_m x^m = f(x) a_m$ y, por lo tanto, $f(x) = x^m$. Si ahora, en el caso general se hace $g(x) = f(x \cdot E)$ entonces, $g(xy) = g(x) g(y)$. De aquí y de la legitimidad de la afirmación cuando $n = 1$ se deduce, que $g(x) = x^s$. Como $X \cdot X^{\vee} = (\det X) \cdot E$, entonces,

$$f(X) f(X^{\vee}) = f((\det X) E) = g(\det X) = (\det X)^s.$$

Pero, $f(X)$, $f(X^{\vee})$ y $\det X$, son polinomios de x_{ij}, $1 \leqslant i, j \leqslant n$, además, $\det X$ es irreducible (véase el ejercicio 7, § 3, cap. 5). Según el teorema 2 sobre la factorizabilidad del anillo de los polinomios de cualquier número de variables $f(X) = c (\det X)^m$, c es la constante, además, $f(XY) = f(X) f(Y) \Rightarrow c^2 = c$ y como $c \neq 0$, entonces, $c = 1$.)

10. Mostrar que el anillo $Q_M(\mathbb{Z})$ de todos los números racionales a/b con «b» no divisible por un número primo dado p (véase el ejercicio 6, § 4, cap. 5), contiene el ideal máximo único

$$J = \{a/b \in Q_M(\mathbb{Z}) \mid p \text{ divide a } a\}.$$

Todo anillo que posea un ideal máximo único, se denomina anillo local. (*Indicación*. Es evidente, que J es ideal propio en $Q_M(\mathbb{Z})$. Si $c/d \notin J$, entonces $c \notin p\mathbb{Z}$, y en consecuencia, $d/c \in Q_M(\mathbb{Z})$. Esto significa, que cualquier ideal L, obtenido de J mediante el agregado de por lo menos un elemento c/d, contiene $1 = c/d \cdot d/c$ y, por lo visto, coincide con $Q_M(\mathbb{Z})$.)

11. Mostrar que en cualquier anillo local K con ideal máximo m, los elementos que no pertenecen a m son reversibles.

12. El ideal R del anillo K con unidad se llama primo, si el factoranillo K/R es de integridad. Todo ideal máximo es primo. El complemento $M = K \setminus R$ a R en el anillo K, es un subconjunto multiplicativo (un monoide que no contiene 0). El anillo $Q_M(K)$ en estas condiciones también se designa por medio del símbolo $M^{-1}K$ o, sencillamente, K_R. Mostrar, que el anillo K_R es siempre local y que su ideal máximo m_R se compone de primos del tipo de a/b, donde $a \in R$ y $b \in K \setminus R$. Mostrar también, que $m_R \cap K = R$.

La operación del paso de K al anillo local K_R se llama *localización del anillo* K *con respecto al ideal primo* R.

§ 3. MÓDULOS

El concepto de módulo sirve de portador de un principio fundamental, elaborado en el álgebra hace medio siglo. Este principio consiste en que, objeto de estudio de cualquier sistema algebraico debe ser no sólo las propiedades internas de este sistema, sino también todas sus representaciones (en el sentido más amplio de esta palabra).

1. Informaciones iniciales sobre módulos. Comencemos con la definición clásica. Sean, K, un anillo asociativo con unidad, y V, un grupo abeliano escrito aditivamente. Sea, luego, dada la aplicación $(x, v) \mapsto xv$ de $K \times V$ en V, que cumple las condiciones:

$$\begin{aligned} &(M1) \quad x(u + v) = xu + xv, \\ &(M2) \quad (x + y)v = xv + yv, \\ &(M3) \quad (xy)v = x(yv), \\ &(M4) \quad 1 \cdot v = v \end{aligned}$$

para todos los $x, y \in K$, $u, v \in V$. Entonces V se llama *K-módulo por la izquierda* (o *módulo por la izquierda sobre el anillo K*). Análogamente se define el K-módulo por la derecha. En adelante, hablaremos sencillamente sobre el K-módulo, aunque en algunas situaciones ambas variedades de módulos aparecen juntas.

El axioma (M4) (condición *de la unitariedad* del módulo), evidentemente, es superfluo, si el anillo K no tiene unidad. Resulta más esencial el hecho de que son posibles modificaciones del axioma (M3), adaptadas a algunos anillos no asociativos. Un ejemplo de módulo sobre un anillo no asociativo se da al final del parágrafo siguiente. Por el momento, partiremos de la definición dada más arriba.

Sea V un K-módulo. El subgrupo $U \subset V$ se llama *submódulo* en V, si $xu \in U$ para todos los $x \in K$, $u \in U$.

Sean, luego, U y V dos K-módulos arbitrarios. Se llama *homomorfismo del K-módulo* (o, sencillamente, *K-homomorfismo*) de U en V, la aplicación $\sigma: U \to V$, tal, que

$$\sigma(u_1 + u_2) = \sigma(u_1) + \sigma(u_2),$$
$$\sigma(xu) = x\sigma(u)$$

para todos los $u_1, u_2, u \in U$, $x \in K$. Se comprueba fácilmente, que $\operatorname{Ker} \sigma = \{u \in U \mid \sigma(u) = 0\}$ es K módulo en U, y la imagen $\operatorname{Im} \sigma$ es K-módulo en V.

Con todo submódulo $U \subset V$ sobre K, se asocia el *módulo cociente* $V/U = \{v + U \mid v \in V\}$ (grupo cociente de un grupo abeliano aditivo) con la operación K, definida según la regla

$$x(v + U) = xv + U.$$

El teorema fundamental sobre los homomorfismos y los dos teoremas sobre los isomorfismos, que demostramos para los grupos (§ 3, cap. 7), y luego para los anillos, se trasladan literalmente, con pequeños cambios en las demostraciones, a los módulos.

Luego del § 2, cap. 7, donde se examinaron los axiomas del tipo (M3), (M4), y luego del fundamental cap. 8 sobre las representaciones de grupos (axiomas (M1), (M3), (M4)), los ejemplos de K-módulos que expondremos, es poco probable que provoquen la sensación de novedad. No obstante, vale la pena considerarlos y compararlos entre sí.

1) Todo grupo abeliano A es $\mathbb{Z}$-módulo. Precisamente, la aplicación $(n, a) \mapsto na$ de $\mathbb{Z} \times A$ en A, satisface todos los axiomas (M1) — (M4). Mirar los grupos abelianos como módulos sobre $\mathbb{Z}$ resulta muy útil.

2) Todo grupo abeliano A es módulo sobre su *anillo de endomorfismos* End A. Por definición, End A se compone de todas las aplicaciones $\varphi: A \to A$ que cumplen la condición $\varphi(a + a') = \varphi(a) + \varphi(a')$. Las operaciones de suma y multiplicación, se introducen en End A de un modo natural: $(\varphi + \psi)(a) = \varphi(a) + \psi(a)$, $(\varphi\psi)(a) = \varphi(\psi(a))$, $1(x) = x$, $0(x) = 0$. La aplicación $(\varphi, a) \mapsto \varphi(a)$ de End $A \times A$ en A dota, evidentemente, a A de la estructura de End A-módulo.

3) El espacio vectorial V sobre el campo P es, sin duda, P-módulo. Si además nos es dado el operador lineal $\mathcal{A}: V \to V$, entonces, le otorgamos a V una estructura de módulo $V_{\mathcal{A}}$ sobre el anillo de los polinomios $P[X]$, haciendo,

$$f(X)v = f(\mathcal{A})v = \alpha_0 v + \alpha_1 \mathcal{A}v + \ldots + \alpha_k \mathcal{A}^k v$$

para cualquier $v \in V$ y cualquier polinomio $f \in P[X]$. Los axiomas (M1) — (M4) se cumplen, por cuanto, juntamente con $\mathcal{A}$ el operador $f(\mathcal{A})$ también será lineal, y

$$(f + g)(\mathcal{A}) = f(\mathcal{A}) + g(\mathcal{A}),$$
$$(fg)(\mathcal{A}) = f(\mathcal{A})\, g(\mathcal{A})$$

(propiedad universal de los anillos de los polinomios; véase § 2, cap. 5). Los subespacios $\mathcal{A}$-invariantes servirán de submódulos en $V_{\mathcal{A}}$. A diferentes operadores lineales de un mismo espacio V les corresponden, hablando en general, distintos (no isomorfos) $P[X]$-módulos.

4) Un ideal por la izquierda, arbitrario, J del anillo K, está provisto de la estructura natural de K-módulo con operación $(x, y) \mapsto xy$, $x \in K$, $y \in J$, inducida por la multiplicación en K. Cuando $J = K$, el anillo K se considera como el módulo K sobre sí mismo. Esta concepción de K lleva a resultados fructíferos.

5) Volviendo al ejemplo anterior, construimos el módulo cociente $K/J = \{y + J \mid y \in K\}$. De acuerdo con la definición general,

$(x, y+J) \mapsto xy + J$, es la operación K en K/J. Observemos, que el epimorfismo canónico π: $K \twoheadrightarrow K/J$, siendo homomorfismo de K-módulos, cumple la relación $\pi(xy) = xy + J = x(y + J) = x\pi(y)$. Si J es un ideal por ambos lados, entonces, K/J es un anillo y π resulta ser homomorfismo de los anillos: $\pi(xy) = \pi(x) \times \pi(y)$. •

La *intersección* $\bigcap_i V_i$ de cualquier familia de *submódulos* $V_i \subset V$ sobre K, es submódulo en V. En particular, la intersección de todos los submódulos, contenedores del conjunto dado $T \subset V$, leva al *submódulo* $\langle T \rangle$, *engendrado por el conjunto* T y compuesto de todos los elementos posibles del tipo $x_1t_1 + \ldots x_kt_k$, donde $x_i \in K$, $t_i \in T$. Observamos, a propósito, que los elementos no nulos $t_1, \ldots, t_k \in V$ se llaman *linealmente dependientes sobre* K, si $x_1t_1 + \ldots + x_kt_k = 0$, donde no todos los $x_i = 0$. El submódulo, engendrado por la familia $\{V_1, \ldots, V_m\}$ de submódulos V_i, se llama *suma* de los mismos y se designa del modo habitual: $\sum V_i = V_1 + \ldots + V_m$.

El módulo V sobre K, engendrado por un elemento único v, se llama *cíclico*. El tiene la forma $V = Kv = \{xv \mid x \in K\}$, donde $v \in V$, y es análogo del grupo cíclico. En particular, el módulo cíclico ${}_KK = K \cdot 1$ (véase el ejemplo 4) es análogo del grupo $(\mathbb{Z}, +)$.

Si $V = Kv_1 + \ldots + Kv_n$, es la suma de un número finito de módulos cíclicos, entonces, el módulo V se llama *engendrado finito*, o *K-módulo de tipo finito*.

Se comprueba fácilmente, que la aplicación $x \mapsto x\,v$ es homomorfismo de los módulos ${}_KK \twoheadrightarrow Kv$. Su núcleo Ann (v) = Ann $(v) = \{x \in K \mid xv = 0\}$ es un ideal por la izquierda en K llamado *anulador* (o *torsión*) del elemento v. De este modo, $Kv \cong K/\mathrm{Ann}\,(v)$. El elemento $v \in V$, con Ann $(v) \neq 0$, se llama *periódico*. El módulo, todos los elementos del cual son periódicos, también se llama *periódico*. Si el módulo V no contiene ningún elemento periódico no nulo, entonces, se dice que V es *módulo sin torsión*.

Se denomina *anulador* (o *torsión*) del K-módulo V, el conjunto

$$\mathrm{Ann}\,(V) = \{a \in K \mid aV = 0\} = \bigcap_{v \in V} \mathrm{Ann}\,(v).$$

Se dice que un módulo es *exacto*, si Ann $(V) = 0$.

A estos mismos conceptos podemos llegar por otro camino. Sea $V(x)$ el conjunto de los elementos $v \in V$ anulados por el elemento $x \in K$. Si K es un anillo íntegro, entonces, $V(x) + V(y) \subset V(xy)$, y tiene sentido el concepto de *submódulo de torsión* Tor $(V) = \sum_{x \in K} V(x)$. En el caso de la igualdad Tor $(V) = V$, se dice que V es *módulo de torsión*. Si Tor $(V) = 0$, entonces, nuevamente llegamos al concepto de módulo sin torsión.

Ejemplos característicos de módulos periódicos: a) todo grupo abeliano finito (módulo periódico de tipo finito sobre $\mathbb{Z}$; torsión $m\mathbb{Z}$, o, simplemente, índice del grupo m); b) el módulo $V_{\mathcal{A}}$ sobre $P[X]$, asociado con el operador lineal $\mathcal{A}$ (véase el ejemplo 3; la torsión, es el ideal principal, engendrado por el polinomio mínimo del operador $\mathcal{A}$).

PROPOSICION 1. *Ann (V) siempre es un ideal por ambos lados del anillo K. Haciendo $(x + \text{Ann}(V))\, v = xv$, le proporcionamos a V la estructura de $(K/\text{Ann}(V))$-módulo exacto.*

DEMOSTRACION. Hagamos $A = \text{Ann}(V)$. Es claro, que A es un subgrupo aditivo en K. Luego $(xax')\, v = xa\, (x'v) = (xa)\, v' = x\, (av') = x \cdot 0 = 0$ para cualesquiera $x,\ x' \in K$, $a \in A$, $v \in V$, de donde se deduce, que $KAK \subseteq A$, o sea, A es un ideal por ambos lados en K. Si ahora, $x + A = x' + A$, entonces, $x - x' \in A$, de donde, $(x - x')\, v = 0$, ó $xv = x'v$. Por lo tanto, $(x + A)\, v = (x' + A)\, v$ o sea, la operación del anillo cociente K/A en V está definida correctamente. Es fácil comprobar, que respecto a esta operación, V es K/A-módulo. Finalmente,

$$(x + A)\, V = 0 \Rightarrow x + A \in \text{Ann}_{K/A}(V) \Rightarrow xV = 0 \Rightarrow x \in A.$$

En consecuencia, sólo el elemento nulo en K/A anula V. ∎

De la proposición 1 se deduce, que el anillo cociente $K/\text{Ann}(V)$ es isomorfo al subanillo del anillo End (V) (véase el ejemplo 2).

Si V, W, son dos K-módulos, entonces, el conjunto $\text{Hom}_K(V,\ W)$ de todos los homomorfismos K-lineales $\sigma\colon V \to W$, resulta ser grupo abeliano respecto a la operación de suma corriente de los homomorfismos:

$$(\sigma + \tau)\, (xv) = \sigma\, (xv) + \tau\, (xv) = x\sigma\, (v) + x\tau\, (v) = \\ = x\, (\sigma\, (v) + \tau\, (v)) = x\, ((\sigma + \tau)\, (v)).$$

Para los módulos V, W, sobre el anillo conmutativo K, el conjunto $\text{Hom}_K(V,\ W)$ resulta ser K-*módulo*, si, como $x\sigma$, $x \in K$, $\sigma \in \text{Hom}_K(V,\ W)$ se entiende la aplicación $v \mapsto x\, (\sigma\, (v))$:

$$(x\sigma)\, (yv) = x \cdot \sigma\, (yv) = x\, (y\sigma\, (v)) = (xy)\, (\sigma\, (v)) = \\ = (yx)\, (\sigma\, (v)) = y\, (x\sigma\, (v)) = y\, ((x\sigma)\, (v)).$$

Cuando $W = V$, el conjunto $\text{End}_K(V) = \text{Hom}_K(V,\ V)$ es un anillo; sirve de multiplicación la composición natural de K-homomorfismos $\varphi \circ \psi\ (\varphi \circ \psi)\, (xv) = \varphi\, (\psi\, (xv)) = \varphi\, (x\psi\, (v)) = x\varphi \times \times (\psi\, (v)) = x\, ((\varphi \circ \psi)\, (v))$. Hay que tener en cuenta, que al considerar V como grupo abeliano aditivo, escribimos $\text{End}_{\mathbb{Z}}(V)$ y, hablando en general, $\text{End}_K(V)$ es subanillo propio en $\text{End}_{\mathbb{Z}}(V)$. En caso de espacio vectorial V sobre el campo K, habitualmente se escribe $\mathcal{L}(V) = \text{End}_K(V)$, llamándolo *anillo* (o *álgebra*) *de operadores lineales*.

El anillo $\text{End}_K(V)$ de K-endomorfismos del módulo V también es llamado *centralizador del anillo K en V*. Su papel es especialmente destacado en el caso de *módulos irreducibles* (o *primos*). El módulo V sobre el anillo K se denomina irreducible, si: a) $V \neq 0$; b) 0, V, son los únicos submódulos en V, y c) $KV \neq 0$ (esta condición se cumple automáticamente, si K contiene la unidad). Es claro, que el *K-módulo $V \neq 0$ es irreducible si, y sólo si, $V = Kv$ es módulo cíclico para cualquier $v \neq 0$ de V.*

PROPOSICION 2 (lema de Schur). *Si V, W, son dos K-módulos irreducibles, y σ es K-homomorfismo no nulo de V en W, entonces, σ es isomorfismo. Luego,* $\text{End}_K(V)$ *es un anillo con división (cuerpo) para cualquier K-módulo V irreducible.*

DEMOSTRACION. Véase el § 4 del cap. 8, donde este mismo lema de Schur (teorema 1) está demostrado para los G-espacios irreducibles. ∎

2. Módulos libres. Llamamos K-módulo V (interno), la *suma directa de sus submódulos* $V_1, \ldots, V_n$, si $V = V_1 + \ldots + V_n$ y $V_i \cap \sum_{j \neq i} V_j = 0$, para $i = 1, \ldots, n$. En otras palabras, $V = V_1 \oplus \ldots \oplus V_n$ (notación de la suma directa de submódulos), si cualquier elemento $v \in V$ se escribe de un modo único en forma de combinación lineal $v = v_1 + \ldots + v_n$, $v_i \in V_i$. La *suma directa exterior de K-módulos* $v_1, \ldots, v_n$ se determina evidentemente (como en el caso de anillos) con la operación $x(v_1, \ldots, v_n) = (xv_1, \ldots, xv_n)$ del elemento $x \in K$ en la fila $(v_1, \ldots, v_n)$, $v_i \in V_i$.

Sean, luego, V, un K módulo, y $\{v_1, \ldots, v_n\}$, un subconjunto finito en V. Se dice, que $\{v_1, \ldots, v_n\}$ *engendra V libremente*, si $V = Kv_1 + \ldots + Kv_n$, y cada aplicación φ del conjunto $\{v_1, \ldots, v_n\}$ en algún K-módulo W, se continúa hasta el K-homomorfismo $\bar{\varphi}: V \to W$, de modo tal, que $\bar{\varphi}(v_i) = \varphi(v_i)$, $1 \leqslant i \leqslant n$.

El módulo V sobre K, libremente engendrado por cierto subconjunto $\{v_1, \ldots, v_n\}$, se llama *módulo libre*, y $\{v_1, \ldots, v_n\}$, es su *base (libre) sobre K*.

PROPOSICION 3. *Son equivalentes las afirmaciones:*

(i) el *conjunto $\{v_1, \ldots, v_n\}$ engendra V libremente;*

(ii) el *conjunto $\{v_1, \ldots, v_n\}$ es linealmente independiente y $\langle v_1, \ldots, v_n\rangle = V$;*

(iii) *cada elemento $v \in V$ se escribe unívocamente en la forma $v = \sum x_i v_i$, $x_i \in K$;*

(iv) *$V = Kv_1 \oplus \ldots \oplus Kv_n$ es una suma directa, y* Ann $(v_i) = 0$;

(v) *$V \cong {}_KK \oplus \ldots \oplus {}_KK$ es la suma directa de n ejemplares ${}_KK$ (de este modo, el K-módulo libre de rango n en relación a la base $\{v_1, \ldots, v_n\}$ es isomorfo al módulo K^n de las filas $(x_1, \ldots, x_n)$ de longitud n con componentes $x_i \in K$).*

DEMOSTRACION. Esta es cercana a los razonamientos expuestos en

el capítulo 2 para los espacios lineales sobre un campo, pero hay que tener cierto cuidado, ya sea en relación con la no conmutatividad del anillo K, o bien con la existencia de elementos no invertibles en K. ▮

Se tienen ejemplos suficientemente complejos de anillos no conmutativos con $K^m \cong K^n$ para $m \neq n$, pero los anillos conmutativos en este sentido se comportan bien.

PROPOSICION 4. *El rango de un módulo finito engendrado sobre el anillo íntegro K, está determinado unívocamente.*

DEMOSTRACION. Sean, $\{v_1, \ldots, v_n\}$, $\{u_1, \ldots, u_m\}$ dos bases del módulo libre V sobre K. Entonces

$$v_j = \sum_{i=1}^{m} a_{ij} u_i, \quad u_i = \sum_{k=1}^{n} b_{ki} v_k.$$

En virtud de la conmutatividad de K, para las matrices $A = (a_{ij})$ y $B = (b_{ki})$ de dimensiones $m \times n$ y $n \times m$ respectivamente, se obtienen las relaciones

$$AB = E_m, \quad BA = E_n.$$

Incluyendo K en el campo de relaciones $Q(K)$, obtendremos, mediante el teorema 4, § 4, cap. 2, (cierto para cualquier campo y no sólo para $\mathbb{R}$), que $\min(n, m) \geqslant m$, $\min(n, m) \geqslant n$, de donde, $m = n$. Agreguemos, que el caso $m < \infty$, $n = \infty$ es imposible, por cuanto en las expresiones de u_i sólo hay un número finito de elementos básicos v_k, que engendran libremente todo el módulo V. ▮

OBSERVACION. En caso de un anillo conmutativo arbitrario K con unidad, se obtendrá el mismo efecto si se elige en K cierto id máximo J y se pasa al campo K/J. Obviamos los detalles.

Observemos que, a diferencia de la situación en los espacios vectoriales, el conjunto engendrador del K-módulo libre, tomado arbitrariamente, no contiene necesariamente la base del módulo Por ejemplo, dos números primos distintos p, q, siempre engendran $_{\mathbb{Z}}\mathbb{Z}$, por cuanto $up + vq = 1$ para algunos $u, v \in \mathbb{Z}$. Pero, $\{p, q\}$ no es la base, puesto que $p \cdot q - q \cdot p = 0$, y $\mathbb{Z}p$, $\mathbb{Z}q$ son submódulos propios en $_{\mathbb{Z}}\mathbb{Z}$.

El papel de los módulos libres está programado en la definición de los mismos.

TEOREMA 1. *Cada K-módulo de tipo finito, es imagen homomorfa de un K-módulo libre de tipo finito.*

DEMOSTRACION. Sea $U = \sum_{i=1}^{n} Ku_i$, un K-módulo engendrado por n elementos $u_1, \ldots, u_n$. Tomemos un K-módulo libre V con base $\{v_1, \ldots, v_n\}$. Su existencia está garantizada por la proposición 3 (v). La aplicación φ: $v_i \mapsto u_i$ es continuada, en correspondencia con la definición de módulo libre, hasta el K-homomorfismo $\tilde{\varphi}: V \twoheadrightarrow U$.

La imagen Im $\tilde{\varphi}$ contiene el conjunto engredrador de módulo U y, por lo tanto, todo el módulo U. ∎

No siempre el submódulo de un módulo libre es también libre, incluso si es un sumando directo del módulo. He aquí un ejemplo sencillo. Sean $K = Z_6$, $U = K(2 + 6Z)$, $V = K(3 + 6Z)$. Entonces, $K = U \oplus V$ es suma directa de los K-módulos U, V, ninguno de los cuales es libre: $|K| = 6$, al mismo tiempo que $|U| = 3$, $|V| = 2$.

TEOREMA 2. *Sea $V = Kv_1 \oplus \ldots \oplus Kv_n$ un módulo libre de rango n sobre el anillo K de los ideales principales. Entonces, cada uno de sus submódulos U resulta de rango libre $m \leqslant n$.*

DEMOSTRACION. Sea al principio $n = 1$, o sea, $V \cong K$. Cualquier submódulo $U \subset V$ es isomorfo al ideal en K, y, en consecuencia, $U \cong (u) = Ku$. Si $u = 0$, entonces, $U = 0$ (el submódulo nulo puede considerarse módulo libre de rango nulo). Si $u \neq 0$, entonces, $au \neq 0$ para todo $0 \neq a \in K$, por cuanto K es un anillo íntegro. Por lo tanto, U es un módulo libre (cíclico) de rango 1. Cuando $n > 1$, razonamos por inducción. Consideremos en V el submódulo libre $V' = Kv_2 \oplus \ldots \oplus Kv_n$ de rango $n - 1$. El módulo cociente $\overline{V} = V/V'$ es libre, con generador cíclico $\overline{v_1} = v_1 + V'$. El contiene el submódulo $\overline{U} = (U + V')/V'$. Si $\overline{U} = 0$, entonces, $U \subset V'$ y, por lo tanto, la afirmación del teorema es cierta por presupuesto de la inducción. Pero, si $\overline{U} \neq 0$, el razonamiento expuesto más arriba para el caso $n = 1$, muestra, que $\overline{U}$ posee el generador cíclico $\bar{u}_1 = u_1 + V'$, donde $u_1 \in U$. Si además $U \cap V' = 0$, entonces, $u \in U \Rightarrow \bar{u} = u + V' \in \overline{U} \Rightarrow \bar{u} = a_1\bar{u}_1$, $a_1 \in K \Rightarrow u - a_1u_1 \in V' \Rightarrow u = a_1u_1 \Rightarrow U = Ku_1$, es un módulo libre de rango 1.

Sea, finalmente, $U \cap V' \neq 0$. Por inducción, el submódulo $U \cap V'$ del módulo libre V' de rango $n - 1$, posee la base libre $\{u_2, \ldots, u_m\}$, donde $0 < m - 1 \leqslant n - 1$. Repitiendo casi literalmente los razonamientos efectuados más arriba, nos convencemos, de que $\{u_1, u_2, \ldots, u_m\}$ es K-base libre para U. Efectivamente, $u \in U \Rightarrow \bar{u} = u + V' \in \overline{U} \Rightarrow \bar{u} = a_1\bar{u}_1$, $a_1 \in K \Rightarrow u - a_1u_1 \in U \cap V' \Rightarrow u - a_1u_1 = a_2u_2 + \ldots + a_mu_m \Rightarrow u = a_1u_1 + a_2u_2 + \ldots + a_mu_m$, $m \leqslant n$. De acuerdo con la proposición 3 (ii), es necesario convencernos de la independencia lineal de los generadores $u_1, \ldots, u_m$. Pero, $\sum x_iu_i = 0 \Rightarrow x_i\bar{u}_i = -\sum_{i>0} x_i\bar{u}_i = 0$ en $\overline{V}$. En consecuencia, $x_1 = 0$, por cuanto $\bar{u}_1$ es base en $\overline{V}$, y, como $\{u_2, \ldots, u_m\}$ es base libre en $U \cap V'$, entonces, $x_2u_2 + \ldots + x_mu_m = 0 \Rightarrow x_2 = \ldots = x_m = 0$. ∎

COROLARIO. *Cada submódulo de un módulo de tipo finito sobre el anillo de los ideales principales, es módulo de tipo finito.*

DEMOSTRACION. Se deduce de los teoremas 1, 2 y del segundo teorema sobre el isomorfismo (teorema sobre la correspondencia entre los submódulos). ∎

No es tan difícil obtener la descripción completa de los módulos de tipo finito sobre el anillo K de los ideales principales. Sin embargo, los principales factores que habitualmente estimulan tal descripción (módulos periódicos sobre $\mathbb{Z}$ y sobre $P[X]$; véanse los ejemplos 1 y 3), han caído (véanse, § 5, cap. 7 y el Complemento), y la demostración de la única concepción modular de distintos géneros de problemas, puede hallarse en el listado de literatura complementaria.

3. Elementos enteros de un anillo. Sea K un anillo íntegro. El elemento $t \in K$ se llama *entero* (*entero sobre* $\mathbb{Z}$), si t es raíz del polinomio unitario $X^n + a_1X^{n-1} + \ldots + a_n \in \mathbb{Z}[X]$. En el caso cuando K es una ampliación algebraica finita del campo $\mathbb{Q}$, o K es un campo, engendrado por todos los números algebraicos complejos, se habla sobre *números algebraicos enteros*, referiendo a ellos, naturalmente, todos los elementos de $\mathbb{Z}$. El ejercicio 9, § 4, cap. 6, muestra, que el *número racional t es algebraico entero si, y sólo si,* $t \in \mathbb{Z}$. Si, luego, $a_0u^n + a_1u^{n-1} + \ldots + a_n = 0$, $a_i \in \mathbb{Z}$, entonces, $(a_0u)^n + a_0a_1(a_0u)^{n-1} + \ldots + a_0^n a_n = 0$, y esto significa, que *cualquier número algebraico, multiplicado por el elemento adecuado $a_0 \in \mathbb{Z}$, se transforma en número algebraico entero.*

Recurriendo al caso general, observemos, pue K es cómodo interpretarlo como $\mathbb{Z}$-módulo. Cualesquiera elementos $t_1, t_2, \ldots, t_n \in K$ engendran en K el submódulo $Kt_1 + Kt_2 + \ldots + Kt_n$ de tipo finito. Si, en particular, t es un elemento entero, y $t^n + a_1t^{n-1} + \ldots + a_n = 0$, $a_i \in \mathbb{Z}$, entonces, el subanillo $\mathbb{Z}[t] \subset K$ resulta $\mathbb{Z}$-módulo de tipo finito, por cuanto $\mathbb{Z}[t] = \mathbb{Z}1 + \mathbb{Z}t + \ldots + \mathbb{Z}t^{n-1}$. Recíprocamente, sea $\mathbb{Z}[t]$ un $\mathbb{Z}$-módulo de tipo finito con generadores $v_1, \ldots, v_n \in K$. Entonces, las relaciones

$$tv_i = a_{i1}v_1 + a_{i2}v_2 + \ldots + a_{in}v_n, \quad 1 \leqslant i \leqslant n,$$

con matriz $A = (a_{ij}) \in M_n(\mathbb{Z})$ llevan a la conclusión, que el sistema lineal homogéneo

$$(t - a_{11})x_1 - a_{12}x_2 - \ldots - a_{1n}x_n = 0,$$
$$-a_{n1}x_1 - a_{n2}x_2 - \ldots + (t - a_{nn})x_n = 0,$$

examinado sobre el campo de relaciones $Q(K)$, tiene solución no nula $(x_1, \ldots, x_n) = (v_1, \ldots, v_n)$ (no todos los $v_i = 0$, por cuanto $1 \in \mathbb{Z}[t]$). Esto significa, que el determinante del sistema es igual a cero (véase el cap. 3) y t es raíz del polinomio unitario $f(T) = \det(TE - A)$. Hemos demostrado, que el *elemento $t \in K$ es entero si, y sólo si, el subanillo $\mathbb{Z}[t] \subset K$ es Z-módulo de tipo finito.*

TEOREMA 3. *Los elementos enteros del anillo K, forman en K un subanillo.*

DEMOSTRACIÓN. Sean $u, v \in K$, elementos enteros. Entonces, $\mathbb{Z}[u, v] = \sum_{i \leqslant n, j \leqslant m} \mathbb{Z}u^i v^j$ es $\mathbb{Z}$-módulo de tipo finito. Como $\mathbb{Z}$ es un anillo de ideales principales, el corolario del teorema 2 (o una comprobación inmediata) muestra, que los submódulos $\mathbb{Z}[u - v]$, $\mathbb{Z}[uv]$ también son $\mathbb{Z}$-módulos de tipo finito. De acuerdo con el criterio expuesto más arriba, los elementos $u - v$, uv, deben ser enteros. ∎

EJEMPLO. La raíz ε de cualquier potencia de 1 es, evidentemente, un número algebraico entero. Según el teorema 3, las combinaciones lineales de números enteros de las raíces de 1 también serán números algebraicos enteros. En particular (véase la demostración de la proposición del § 4, cap. 8), los *valores* $\chi_\Phi(g)$, $g \in G$, *del carácter* χ_Φ *de cualquier representación lineal* Φ *sobre* $\mathbb{C}$ *del grupo finito* G, *son números algebraicos enteros.*

4. Sucesiones unimodulares de polinomios. Sea $K = P[X_1, \ldots, X_n]$ un anillo de polinomios de n variables sobre el campo P. La sucesión $[f_1, \ldots, f_r]$ de r polinomios $f_i \in K$ se denomina unimodular, si $Kf_1 + Kf_2 + \ldots + Kf_r = K$, es decir,

$$u_1 f_1 + u_2 f_2 + \ldots + u_r f_r = 1 \tag{1}$$

para ciertos $u_i \in K$, $1 \leqslant i \leqslant r$. Sea, luego, V un módulo de tipo finito sobre K. En relación con ciertas cuestiones delicadas de la geometría algebraica, el matemático francés J. P. Serre (año 1955) formuló la hipótesis:

$$\{V \oplus K^s \cong K^{s+t}\} \Rightarrow V \cong K^t,$$

a la que se le otorgó la siguiente forma elegante: «toda relación (1) puede ser escrita en forma de igualdad

$$\begin{vmatrix} f_1 & f_2 & \ldots & f_r \\ u_{21} & u_{22} & \ldots & u_{2r} \\ \cdot & \cdot & \cdot & \cdot \\ u_{r1} & u_{r2} & \ldots & u_{rr} \end{vmatrix} = 1 \tag{2}$$

para los $u_{ij} \in K$ adecuados».

Esta afirmación, pese a su aparente sencillez, fue demostrada recién en el año 1976, en forma independiente por A. A. Suslin (URSS) y D. Quillen (EE.UU.), aunque el caso particular $n = 1$ se le adjudica a Ch. Hermite (1848). El caso general es más justo.

TEOREMA 4. *Sean,* $a_1, a_2, \ldots, a_r$ $(r \geqslant 2)$ *los elementos distintos de cero del anillo* K *de los ideales principales, y* $d =$ *m.c.d.* $(a_1, \ldots, a_r)$. Entonces, existe la matriz $A \in M_r(K)$ cuya primera fila es $(a_1, a_2, \ldots, a_r)$ y su det $A = d$.

DEMOSTRACIÓN. Nos basamos en los resultados, formulados al final del p. 1 del § 2. Para $r = 2$, escribiendo d en forma $d = u_1 a_1 +$

$+ \ldots + u_2 a_2$ con $u_i \in K$, inmediatamente hallamos la matriz requorida:

$$A = \left\| \begin{matrix} a_1 & a_2 \\ -u_2 & u_1 \end{matrix} \right\|.$$

Utilizando ahora la inducción con respecto a r, representamos a $d' =$ = m.c.d. $(a_1, \ldots, a_{r-1})$ (en la forma $d' = \det A'$, donde $A' \in$ $\in M_{r-1}(K)$ es una matriz con primera fila $(a_1, \ldots, a_{r-1})$. Como $d =$ m.c.d. (d', a_r), entonces, $d' = ud' + va_r$. Introducimos la matriz

$$A = \left\| \begin{array}{ccc:c} & & & a_r \\ & A' & & 0 \\ & & & \vdots \\ & & & 0 \\ \hdashline \frac{-va_1}{d}, & \ldots & \frac{-va_{r-1}}{d} & u \end{array} \right\|.$$

De primera fila de la matriz $A \in M_r(K)$ sirve $(a_1, a_2, \ldots, a_r)$. Descomponiendo el $\det A$ por los elementos de la última columna, hallamos

$$\det A = u \det A' + (-1)^{r+1} a_r \det A'' = ud' + a_r(-1)^{r+1} \det A'', \quad (3)$$

donde A'' es la matriz que se obtiene de A eliminado en ésta la primera fila y la última columna.

Por otra parte, si se multiplica la primera fila de la matriz A' por $-v$, y se coloca el producto en el último lugar en A', conservando el orden de las restantes filas (lo que se logra mediante permutaciones sucesivas), entonces se obtiene la matriz A''', que aparece en el caso en que multiplicamos la última fila de A'' por d'. Esto significa que,

$$d' \det A'' = \det A''' = (-1)^{r-1} v \det A' = (-1)^{r-1} vd'.$$

Reemplazamos con esta expresión en la relación obtenida de (3) al multiplicar ambos miembros de ella por d':

$$d' \det A = u(d')^2 + a_r(-1)^{r-1} d' \det A'' =$$
$$= u(d')^2 + a_r(-1)^{r+1}(-1)^{r-1} d'v = d'(ud' + va_r),$$

y, simplificando d', llegamos a la representación requerida

$$d = ud' + va_r = \det A. \quad \blacksquare$$

Para $n > 1$ la idea fundamental consiste en el estudio de la acción del grupo $GL(r, P[X_1, \ldots, X_{n-1}])$ en el conjunto de las sucesiones unimodulares y en los razonamientos que utilizan la inducción según n. La demostración puede encontrarse en el artículo original (Суслин А. А., Проективные модули над кольцом многочленов свободны, ДАН СССР, 229, №5 (1976), 1063-1066) (Suslin A. A.,

Módulos proyectivos libres sobre el anillo de los polinomios) o por la intervención en el seminario de N. Bourbaki (Ferrand D., Sém. N. Bourbaki, 28 ème année, 1975/76, Juin 1976). La exposición es muy sencilla. Acerca de las dificultades para lograr esta demostración, se puede juzgar por una intervención anterior en el seminario de N. Bourbaki (Bass H., N. Bourbaki, 26 ème année, 1973/74, Juin, 1974). En la literatura indicada se encuentran planteos de problemas no resueltos. Todo este círculo de cuestiones es muy interesante para las discusiones en los seminarios especializados.

§ 4. ALGEBRAS SOBRE UN CAMPO

1. Definición y ejemplos de álgebras. Hasta ahora no dimos gran importancia al hecho de que casi todos los anillos que conocemos tienen a un mismo tiempo estructura de espacio vectorial sobre un campo.

DEFINICION. Se llama *álgebra* (o *álgebra lineal*) sobre el campo P, al par constituido por el anillo $(A, +, \cdot)$ y el espacio vectorial A sobre P (el conjunto básico A del anillo y el espacio vectorial, es lo mismo; también son idénticas las operaciones de suma $+$ y el elemento nulo 0). Además,

$$\lambda (xy) = (\lambda x) y = x (\lambda y)$$

para todo $\lambda \in P$, x, $y \in A$. El álgebra se llama *asociativa*, si es asociativo el anillo $(A, +, \cdot)$. La dimensión del espacio vectorial A sobre P, también se llama *dimensión del álgebra* A.

A las álgebras se trasladan, con puntualizaciones insignificantes, los principales conceptos de la teoría de anillos. Así, se considera *subálgebra* del álgebra A, cualquier subanillo $B \subset A$, que sea a un mismo tiempo subespacio del espacio vectorial A. Si T es un subconjunto en A, entonces, la subálgebra $P[T]$ engendrada por él, es la intersección de todas las subálgebras en A, contenedoras de T. Análogamente se definen los ideales y las *álgebras cocientes* respecto a ellos. De *homomorfismos de álgebras* sirven los homomorfismos de anillos que, a un mismo tiempo, son aplicaciones P-lineales.

El *centro* $Z(A)$ *del álgebra asociativa* A se define como el conjunto de todos los elementos $a \in A$, permutados con cada elemento de A: $a \in Z(A) \Leftrightarrow ax = xa$, $\forall x \in A$. Evidentemente, $(a - a')x = ax - a'x = xa - xa' = x(a - a')$, $(aa')x = a(a'x) = a(xa') = (ax)a' = x(aa')$, $(\lambda a)x = \lambda(ax) = \lambda(xa) = x(\lambda a)$, para todos los a, $a' \in Z(A)$, $\lambda \in P$. Por eso, el centro $Z(A)$ es subálgebra en A. La igualdad $Z(A) = A$ tiene lugar si, y sólo si, A es un álgebra conmutativa.

Si A es un álgebra asociativa con unidad 1, entonces, inmediatamente se comprueba, que $\lambda \cdot 1 \in Z(A)$, además, la correspondencia

$\lambda \mapsto \lambda \cdot 1$, $\forall \lambda \in P$, determina la aplicación monomorfa de P en A. En este sentido, se puede entender como álgebra A, el anillo A junto con el subcampo separado, contenido en el centro $Z(A)$.

Pongamos algunos ejemplos de álgebras.

1) La ampliación $F \supset P$ de grado finito $[F : P]$ del campo P es, evidentemente, un álgebra asociativa y conmutativa (con unidad) de dimensión finita $\dim_P F = [F : P]$. Hemos utilizado ya este hecho en el § 1.

2) El anillo de los polinomios $K = P[X_1, \ldots, X_n]$ con coeficientes en el campo P tiene la estructura natural de un álgebra asociativa, conmutativa, infinitadimensional, sobre el campo P. Observemos, que

$$K = K_0 \oplus K_1 \oplus K_2 \oplus \ldots$$

es la suma directa de subespacios vectoriales finitodimensionales K_m de polinomios homogéneos de grado m ($K_0 = P$), siendo $K_i K_j \subset \subset K_{i+j}$. Las álgebras de tipo semejante, se llaman *graduadas*.

3) El álgebra conmutativa $X_{\mathbb{C}}(G)$ con unidad χ_1, engendrada sobre $\mathbb{C}$ por todos los caracteres del grupo finito G, tiene la dimensión r, igual al número de clases de los elementos conjugados en G (teorema 2, § 7, cap. 8).

4) El anillo $M_n(P)$ de las matrices cuadradas de orden n con coeficientes en el campo P, es un álgebra de dimensión n^2 sobre P. Los elementos básicos $\{E_{ij} \mid i, j = 1, 2, \ldots, n\}$ del álgebra $M_n(P)$ se multiplican de acuerdo con la regla $E_{ik}E_{lj} = \delta_{kl}E_{ij}$. De acuerdo con el teorema 3, § 3, cap. 2, el centro $Z(M_n(P)) = \{\lambda E\} \cong P$.

El álgebra asociativa A con unidad, se denomina *simple central sobre el campo P*, si $Z(A) \cong P$ y en A no hay ideales por ambos lados, distintos de 0 y A.

PROPOSICION 1. *$M_n(P)$ es un álgebra central simple.*

Sea J un ideal en $M_n(P)$ diferente del nulo, y sea

$$0 \neq a = \sum \alpha_{ij} E_{ij} \in J.$$

Si $\alpha_{kl} \neq 0$, entonces, $E_{st} = \alpha_{kl}^{-1} E_{sk} \cdot a \cdot E_{lt} \in J$ para cualesquiera $s, t = 1, \ldots, n$ y, por lo tanto, $J = M_n(P)$.

Una afirmación análoga es legítima para el álgebra matricial completa $M_n(D)$ sobre el cuerpo arbitrario D. El extraordinariamente importante *teorema* de *Vedderbarn* (en un contexto más amplio, *teorema de Vedderbarn—Artin*) enuncia que, recíprocamente, *todo álgebra simple, asociativa y finitadimensional sobre el campo P, es isomorfa a $M_n(D)$, donde el número natural n está determinado unívocamente, y el cuerpo D (que es un álgebra de dimensión finita sobre P) con exactitud hasta el isomorfismo.*

El álgebra matricial $M_n(P)$ posee también la propiedad universal siguiente.

PROPOSICION 2. *Todo álgebra asociativa n-dimensional A, sobre el campo P, es isomorfa a cierta subálgebra en $M_k(P)$, donde $k \leqslant n+1$.*

DEMOSTRACION. Consideraremos que A es un álgebra con 1 y la incluimos en $M_n(P)$. Con este fin, a cada elemento $a \in A$ le ponemos en correspondencia el operador lineal L_a: $x \mapsto ax$ en el espacio vectorial A. La linealidad de L_a es consecuencia de la bilinealidad de la operación de multiplicación en A. Como, evidentemento, $L_{\lambda a} = \lambda L_a$, $L_{a+b} = L_a + L_b$, $L_{ab} = L_a L_b$ (lasociatividadl) y $L_1 = \mathscr{E}$, entonces, la aplicación φ: $a \to L_a$ es un homomorfismo. Su inyectividad se asegura debido a la existencia del elemento unidad: $a \neq 0 \Rightarrow L_a \cdot 1 = a \cdot 1 = a$, $L_a \neq 0$.

Sea ahora A un álgebra sin unidad. Incluyamos en la consideración el espacio vectorial $\tilde{A} = P \oplus A$ y definemos sobre el mismo la multiplicación, haciendo $(\lambda, a)(\lambda', a') = (\lambda\lambda', aa' + \lambda a' + \lambda' a)$. Se comprueba fácilmente, que con esta ley de multiplicación $\tilde{A}$ resulta álgebra sobre P con elemento unitario $(1, 0)$.

Como $\dim_P \tilde{A} = \dim_P \tilde{A} + 1 = n + 1$, entonces, el rozamiento anterior permite incluir $\tilde{A}$, y, conjuntamente, A en $M_{n+1}(P)$.

No es difícil observar una similitud total en las demostraciones de la proposición 2 y del teorema de Cayley para los grupos finitos. En ambos casos se utiliza una representación regular. En forma más general, se entiende como *representación del álgebra A* sobre P, cualquier homomorfismo $A \to \mathfrak{L}(V) = \mathrm{End}_F(V)$, donde $F \supset P$ es cierta ampliación del campo P. En otras palabras, el espacio vectorial V sobre F es abastecido de una estructura de A-módulo por la izquierda, en el sentido de las definiciones del § 3, además,

$$(\lambda x)\cdot v = x\cdot(\lambda y), \quad \forall \lambda \in P,\ x \in A,\ v \in V.$$

Eligiendo en V alguna base, llegaremos, como en el caso de los grupos, a la representación matricial $A \to M_r(F)$, donde $r = \dim_F(V)$.

2. Algebras con división (cuerpos). Como muestra el teorema de Vedderbarn, formulado más arriba, el estudio de las álgebras con división es una parte constitutiva importante de la teoría estructural general de las álgebras asociativas. El lema de Schur (proposición 3, § 3) también confirma esta consideración. Antes de exponer algunos resultados sobre las álgebras con división, nos detenemos en una afirmación auxiliar.

PROPOSICION 3. *En el álgebra asociativa A (con elemento unidad 1) de dimensión n sobre el campo P, cada elemento $a \in A$ es raíz del polinomio $f_a \in P[X]$* de grado $\leqslant n$. El elemento $a \in A$ es invertible con exactitud, cuando $f_a(0) \neq (0)$. *Si en A no hay divisores de cero, entonces, A es un álgebra con división. Si el campo P es algebraicamente cerrado, entonces, $n = 1$, $A = P$.*

DEMOSTRACIÓN. En virtud de que A es finitadimensional, los elementos $1, a, a^2, \ldots$ no pueden ser todos linealmente independientes sobre P. Por lo tanto, existe un polinomio unitario $f_a(X) = X^m + \alpha_1 X^{m-1} + \ldots + \alpha_m \neq 0$ del menor grado $m \leqslant n$, con coeficientes $\alpha_i \in P$, tal, que $f_a(a) = 0$. Si $\alpha_m \neq 0$, entonces, la relación $f_a(a) = 0$, reescrita en la forma $[-\alpha_m^{-1}(a^{m-1} + \alpha_1 a^{m-2} + \ldots + \alpha_{m-1})]\, a = 1$, muestra, que a es un elemento invertible. Recíprocamente, supongamos, que $a \in A$ no es divisor de cero, pero $\alpha_m = 0$. Entonces,

$$(a^{m-1} + \alpha_1 a^{m-2} + \ldots + \alpha_{m-1})\, a = 0 \Rightarrow a^{m-1} + \alpha_1 a^{m-2} + \ldots + \alpha_{m-1} = 0,$$

lo que contradice la minimalidad de $f_a(X)$. En consecuencia, $\alpha_m \neq 0$. En particular, todos los elementos en A, que no son divisores de cero, son invertibles.

Si el campo P es algebraicamente cerrado, entonces, $f_a(X) = (X - c_1) \ldots (X - c_m)$, $c_i \in P$, de donde, $(a - c_1)\, b = 0$, $b = (a - c_2) \ldots (a - c_m) \neq 0$. La ausencia de divisores de cero en A deja una sola posibilidad: $m = 1$ y $a - c_1 = 0$, $a = c_1 \in P$. Como esto es cierto para cualquier elemento $a \in A$, entonces, $A = P$. ∎

Vemos, que las propiedades de las álgebras con división dependen fundamentalmente del campo básico P. Naturalmente, en todo tiempo las álgebras con división sobre el campo de los números reales $\mathbb{R}$ despertaron un interés especial. La existencia del campo $\mathbb{C} = \mathbb{R} + i\,\mathbb{R}$ daba motivo para la búsqueda de otros « sistemas hipercomplejos ». Estas búsquedas culminaron triunfalmente en el año 1843, cuando Hamilton formuló su famosa álgebra de cuaterniones reales.

EJEMPLO (álgebra de los cuaterniones $\mathbb{H}$). Formalmente,

$$\mathbb{H} = \mathbb{R} + i\mathbb{R} + j\mathbb{R} + k\mathbb{R},$$

donde i, j, k, son magnitudes que se multiplican de acuerdo con la regla

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.$$

El elemento $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in \mathbb{H}$ se llama *cuaternión*. Se comprueba, inmediatamente, que $\mathbb{H}$ es un álgebra asociativa con centro $Z(\mathbb{H}) = \mathbb{R}$. Pero, es más conveniente examinar primero el modelo del álgebra $\mathbb{H}$-conjunto $\mathbb{C}$

$$\Phi(\mathbb{H}) = \left\{ \left\| \begin{matrix} a & b \\ -\bar{b} & \bar{a} \end{matrix} \right\| \;\middle|\; a, b, c \in \mathbb{C} \right\} \subset M_2(\mathbb{C}).$$

El ejercicio elemental de las operaciones con matrices muestra que $\Phi(\mathbb{H})$ es un anillo con división. Un ejercicio análogo se analizó en el § 1, cap. 5 cuando se introdujo el campo $\mathbb{C}$. Sólo es necesario recordar, que la multiplicación $\Phi(\mathbb{H})$ no es conmutativa. De acuerdo con las reglas de cálculo de la matriz inversa

$$\left\| \begin{matrix} a & b \\ -\bar{b} & \bar{a} \end{matrix} \right\|^{-1} = \delta^{-1} \left\| \begin{matrix} \bar{a} & -b \\ \bar{b} & a \end{matrix} \right\|,$$

donde

$$\delta = \det \begin{Vmatrix} a & b \\ -\bar{b} & \bar{a} \end{Vmatrix} = a\bar{a} + b\bar{b} \quad (\neq 0 \text{ cuando } a \neq 0 \text{ ó } b \neq 0).$$

A propósito, de aquí se deduce, que el grupo multiplicativo $\Phi(\mathbb{H})^* = \Phi(\mathbb{H}) \setminus \{0\}$ contiene un subgrupo, isomorfo a $SU(2)$ (véase § 1, cap. 7).

Haciendo

$$q_0 = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \quad q_1 = \begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix}, \quad q_2 = \begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}, \quad q_3 = \begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix},$$

observamos, que

$$q_s^2 = -q_0; \ s \neq 0; \ q_1q_2 = q_3 = -q_2q_1, \ q_2q_3 = q_1 = -q_3q_2, \ q_3q_1 = q_2 = -q_1q_3.$$

Se comprende, que la aplicación $\Phi : \mathbb{H} \to \Phi(\mathbb{H})$, definida por la relación $1 \mapsto q_0$, $i \mapsto q_1$, $j \mapsto q_2$, $k \mapsto q_3$, es una representación bidimensional sobre $\mathbb{C}$ del álgebra de los cuaterniones $\mathbb{H}$. Con esto, al cuaternión x le corresponde la matriz

$$\Phi_x = \begin{Vmatrix} a & b \\ -\bar{b} & \bar{a} \end{Vmatrix} = \alpha_0 q_0 + \alpha_1 q_1 + \alpha_2 q_2 + \alpha_3 q_3,$$

donde $a = \alpha_0 + i\alpha_1$, $b = \alpha_2 + i\alpha_3$, $i = \sqrt{-1}$. Las *unidades cuaterniones* i, j, k, engendran en $\mathbb{H}^*$ el grupo, conocido por nosotros de los cuaterniones Q_8, de orden 8, y la limitación $\Phi|_{Q_8}$ nos brinda su representación bidimensional irreducible (véase el final del § 3, cap. 7).

Para cada cuaternión $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ está definido el cuaternión conjugado $x^* = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$ (análogo del número complejo conjugado).

La operación de conjugación tiene las evidentes propiedades siguientes:

$$(x + y)^* = x^* + y^*; \quad x^* = x \Longleftrightarrow x \in \mathbb{R}; \quad x^* = -x \Longleftrightarrow \alpha_0 = 0$$

(x es un «cuaternión puramente imaginario»). El producto $xx^* = N(x)$ se llama *norma del cuaternión* x. Con ayuda de la correspondencia Φ se hace inmediatamente claro, que $(xy)^* = y^*x^*$ y $N(xy) = N(x)N(y)$, además, $N(x) = \det \Phi(x) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$.

El lugar ocupado por los cuaterniones, se revela bien por el *teorema siguiente de Frobenius. Sobre el campo* $\mathbb{R}$ *existen solamente tres álgebras asociativas finitadimensionales con división:* $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$. Para la demostración (en la que no nos detendremos) es esencial, que el polinomio mínimo $f_t(X)$ de cualquier elemento $0 \neq t \in \mathbb{R}$ del álgebra con división D sobre $\mathbb{R}$ debe ser cuadrático (véase la proposición 3 y el teorema 1, § 4, cap. 6).

Hace relativamente poco, en base a razonamientos topológicos profundos, fue demostrado, que *sobre* $\mathbb{R}$ *todo álgebra finitadimensional con división* (*no necesariamente asociativa*) tiene una dimensión 1, 2, 4 u 8. Todas las posibilidades se realizan.

Hace más de 70 años, un buen resultado sobre cuerpos finitos fue obtenido por Vedderbarn, el mismo tiene un significado fundamental para la geometría. Este teorema, directamente relacionado con el contenido del § 1, lo demostraremos ahora.

TEOREMA 1 (Vedderburn). *Cada anillo finito asociativo con división es conmutativo.*

DEMOSTRACIÓN. Sea D un anillo finito con división, Z su centro. Evidentemente, Z es un campo y D un espacio vectorial de dimensiones finitas sobre Z:

$$D = Ze_1 \dot{+} Ze_2 \dot{+} \ldots \dot{+} Ze_n.$$

De acuerdo con los resultados del § 1, $Z = \mathbb{F}_q$ para cierto $q = p^m$, así que $|D| = q^n$. Sea, luego, $x \in D \setminus Z$. Los elementos permutados con x forman el conjunto $C(x) = \{y \in D \mid yx = xy\}$, cerrado con respecto a las operaciones de suma y multiplicación. Con otras palabras, $C(x)$ es una subálgebra con división en D, contenedora de Z. Si q^d es el número de elementos en $C(x)$, entonces, $d = d(x)$ es divisor de n, $d < n$, por cuanto, interpretando D como espacio vectorial por la izquierda

$$D = C(x) f_1 \dot{+} \ldots \dot{+} C(x) f_r$$

sobre $C(x)$, tenemos $q^n = |C(x)|^r = q^{dr}$. Observemos ahora, que Z^* es el centro del grupo multiplicativo D^*, y que $(q^n - 1)/(q^d - 1) = (D^* : C(x)^*)$ es el número de elementos conjugados con x en D^*. Por eso, la fórmula (2′), § 2, cap. 7, toma la forma

$$q^n - 1 = |K^*| = (q-1) + \sum_d \frac{q^n - 1}{q^d - 1}, \qquad (*)$$

donde d recorre cierto conjunto de divisores de n, menores que n. Las propiedades del polinomio circular $\Phi_n(X)$, establecidas en el § 1, muestran (véase el ejercicio 6, § 1), que el número entero $\Phi_n(q)$ divide tanto $q^n - 1$, como también $(q^n - 1)/(q^d - 1)$, para $d \mid n$, $d < n$. En este caso, según $(*)$, $\Phi_n(q) \mid (q - 1)$, y esto implica la igualdad $n = 1$ (véase el ejercicio 7, § 1) y por lo tanto, la conmutatividad $D = Z$. ∎

3. Algebras grupales y módulos sobre ellas. En relación con la representación regular del grupo finito G en el § 1, del cap. 8 se introdujo un espacio vectorial $\langle e_g \mid g \in G\rangle_K$ sobre el campo K. Transformamos ahora al mismo en K-álgebra, haciendo $e_g e_h = e_{gh}$ y extendiendo esta regla respecto a la linealidad, a los « vectores » arbitrarios $\sum \alpha_g e_g$, $\alpha_g \in K$. Para simplificar, habitualmente se reemplaza la escritura de e_g por g y se examina el conjunto $K[G]$ de todas las sumas formales posibles $\sum \alpha_g g$, $\alpha_g \in K$. Por definición, $\sum \alpha_g g = \Sigma \beta_g g_g \Leftrightarrow \alpha_g = \beta_g$, $\forall \in G$. Las operaciones sobre las sumas formales

$$\sum_g \alpha_g g + \sum_g \beta_g g = \sum_g (\alpha_g + \beta_g) g,$$

$$\lambda \left(\sum \alpha_g g\right) = \sum_g \lambda \alpha_g g,$$

$$\left(\sum_g \alpha_g g\right)\left(\sum_h \beta_h h\right) = \sum_{g,h} \alpha_g\beta_h gh = \sum \gamma_u u,$$
$$\text{donde } \gamma_u = \sum_g \alpha_g \beta_{g^{-1}u} \tag{1}$$

dan en $K[G]$ una estructura de álgebra asociativa. Es aceptado denominar $K[G]$ *álgebra grupal del grupo finito G* sobre el campo K. Los elementos básicos del espacio $K[G]$ sirven de sumas formales $1 \cdot g$, $g \in G$, identificables con los elementos $g \in G$; $\dim_K K[G] = |G|$. Así pues, el grupo G se considera incluido en el álgebra $K[G]$. El elemento unidad $e \in G$ es unidad en $K[G]$. En el caso cuando K es anillo asociativo conmutativo con unidad, se obtiene el *anillo grupal* $K[G]$ del grupo G sobre K.

Además, una estructura análoga es aplicable al grupo arbitrario G, no necesariamente finito, si se conviene en considerar solamente la suma $\Sigma\alpha_g g$ con un número finito de coeficientes distintos de cero. Es también cómodo, interpretar a $A = \Sigma\alpha_g g$ como una función en el grupo G (con valores $A(g) = \alpha_g$ en K), igual a cero en casi todos los lugares (o sea, con un número finito de valores diferentes de cero). Con esto, a las fórmulas (1) les responden las operaciones de suma corrientes

$$(A_1 + A_2)(g) = A_1(g) + A_1(g)$$

y el *paquete de funciones*

$$A_3 = A_1 * A_2, \quad A_3(u) = \sum_g A_1(g) A_2(g^{-1}u).$$

La teoría de los anillos grupales, es una extensa parte del álgebra, que tiene problemática propia, pero, para nosotros, $K[G]$ es sólo una ilustración de conceptos generales, introducidos en los últimos dos capítulos.

TEOREMA 2. *Existe correspondencia biunívoca entre los $K[G]$-módulos, que son subespacios vectoriales de dimensiones finitas sobre el campo K, y las representaciones lineales del grupo G.*

DEMOSTRACION. Sea (Φ, V) una representación del grupo G. Continuamos Φ respecto a la linealidad en los elementos de $K[G]$, definiendo

$$\tilde{\Phi}\left(\sum \alpha_g g\right) = \sum \alpha_g \Phi(g),$$

y hacemos

$$\left(\sum \alpha_g g\right) \circ v = \sum \alpha_g \Phi(g) v, \quad \forall v \in V.$$

La operación $\circ$ introduce en V la estructura $K[G]$ — módulo en la acepción corriente de esta palabra. Observemos, que

$$\left(\sum \alpha_g g\right) \circ (\lambda v) = \sum \alpha_g \Phi(g)(\lambda v) = \sum \alpha_g \lambda \Phi(g) v =$$
$$= \lambda\left(\sum \alpha_g \Phi(g) v\right) = \lambda\left(\left(\sum \alpha_g g\right) \circ v\right),$$

o sea, la multiplicación por escalares en V y en $K[G]$ están coordinadas. El par $(\tilde{\Phi}, V)$ es natural denominarlo representante lineal del álgebra $K[G]$.

Recíprocamente, si V es un espacio vectorial sobre K, que resulta ser módulo sobre $K[G]$ con la operación $(\sum \alpha_g g, v) \mapsto (\sum \alpha_g g) \circ v$, entonces, haciendo

$$\tilde{\Phi}(\sum \alpha_g g) v = (\sum \alpha_g g) \circ v,$$

definimos el homomorfismo $\tilde{\Phi}: K[G] \to \mathrm{End}_K(V)$ (o sea, la representación del álgebra $K[G]$), cuya limitación $\Phi = \tilde{\Phi}|_G$ sobre G, nos brinda la representación del grupo G. ∎

En correspondencia con el teorema 1, el espacio de la representación V del grupo G frecuentemente es llamado *módulo de la representación* del grupo G o, brevemente, *G-módulo*. Cambios terminológicos correspondientes, afectan a otros conceptos de la teoría de representaciones.

Sean, luego, G un grupo finito, $K = \mathbb{C}$, el campo de los números complejos. De acuerdo con los resultados del cap. 8, cada G-módulo irreducible sobre $\mathbb{C}$ (o sea, $\mathbb{C}[G]$ = módulo) con carácter χ_i isomorfo a cierto ideal por la izquierda J_i del álgebra $\mathbb{C}[G]$ (véase, en relación con esto, el ejemplo 4, § 3). Si $\dim_{\mathbb{C}} J_i = n_i$, entonces, $\mathbb{C}[G]$ contiene la suma directa $A_i = J_{i,1} \oplus \ldots \oplus J_{i,n_i}$ de n_i ideales por la izquierda, de $\mathbb{C}[G]$-isomorfos $J_i = J_{i,1}$. Eligiendo un representante J_i en cada clase de ideales isomorfos por la izquerda, podemos escribir la descomposición

$$\mathbb{C}[G] = A_1 \oplus A_2 \oplus \ldots \oplus A_r, \tag{2}$$

correspondiente a la descomposición de la representación regular del grupo G. Observemos, que cada uno de los componentes A_i está determinado unívocamente.

Si ahora J es el ideal mínimo por la izquierda del álgebra $\mathbb{C}[G]$ y $t \in \mathbb{C}[G]$, entonces, Jt también es un ideal mínimo por la izquierda (posiblemente, nulo). Por lo tanto, la aplicación $\varphi: J \to Jt$, definida por la relación $v \mapsto vt$ $(v \in J)$, o es nula, o bien $\mathbb{C}[G]$ — isomorfismo, por cuanto $xv \in J$ para cualquier $x \in \mathbb{C}[G]$ y $\varphi(xv) = (xv)t = x(vt) = x\varphi(v)$. Por esta causa, $J \subset A_i \Rightarrow Jt \subset A_i$, $\forall t \in \mathbb{C}[G]$, y, en consecuencia, A_i es un ideal por ambos lados en $\mathbb{C}[G]$. La descomposición (2) es directa, así que

$$i \neq j \Rightarrow A_i A_j \subset A_i \subset A_i \cap A_j = 0.$$

Nos disponemos a obtener una información más exacta sobre la descomposición (2), apoyándonos en la teoría de caracteres, desarrollada en el cap. 8. Primeramente, hallemos el centro $Z(\mathbb{C}[G])$ del álgebra grupal $\mathbb{C}[G]$. Por definición,

$$z \in Z(\mathbb{C}[G]) \Leftrightarrow zg = gz, \ \forall g \in G.$$

Si $z = \sum_{h \in G} \gamma_h h$, entonces,

$$\sum_{t \in G} \gamma_{g^{-1}t} t = g \left(\sum_h \gamma_h h\right) = \left(\sum_h \gamma_h h\right) g = \sum_{t \in G} \gamma_{tg^{-1}} t,$$

de donde, $\gamma_{g^{-1}t} = \gamma_{tg^{-1}}$, $\forall t \in G$. Haciendo $t = gh$, obtendremos $\gamma_h = \gamma_{ghg^{-1}}$. Esto significa, que

$$Z(\mathbf{C}[G]) = \langle z_1, z_2, \ldots, z_r \rangle \mathbf{C},$$

donde

$$z_i = \sum_{g \in g_i^G} g; \quad i = 1, 2, \ldots, r \tag{3}$$

($g_1, g_2, \ldots, g_r$, son representantes de las clases de elementos conjugados del grupo G). Se entiende, que $z_1, z_2, \ldots, z_r$, son elementos linealmente independientes y, por lo tanto, $\dim_{\mathbf{C}} Z(\mathbf{C}[G]) = r$.

A cada elemento $a \in A_i$ le ponemos en correspondiencia el operador lineal $L_a^{(i)}$, que opera en el ideal mínimo por la izquierda $J_i = J_{i,1}$ según la regla $L_a^{(i)}(v) = av$, $v \in J_i$. Como, evidentemente, $L_{\lambda a}^{(i)} = \lambda L_a^{(i)}$, $L_{a+b}^{(i)} = L_a^{(i)} + L_b^{(i)}$, $L_{ab}^{(i)} = L_a^{(i)} L_b^{(i)}$ entonces, φ: $a \to L_a^{(i)}$ es homomorfismo del álgebra A_i en el álgebra de los endomorfismos $\mathrm{End}_{\mathbf{C}} J_i \cong M_{n_i}(\mathbf{C})$. Supongamos, que $0 \neq a \in \mathrm{Ker}\, \varphi$, o sea, $aJ_i = 0$. Todos los ideales por la izquierda $J_{i,j}$ son $\mathbf{C}[G]$ — isomorfos, y, si φ_j: $J_i \to J_{i,j}$ es un isomorfismo, entonces,

$$a J_{i,j} = a\varphi_j(J_i) = a\varphi_j(eJ_i) = \varphi_j(a \cdot eJ_i) = \varphi_j(0) = 0.$$

En consecuencia, $aA_i = aJ_{i,1} + \ldots + aJ_{i,n_i} = 0$, y en tal caso, también $a\,\mathbf{C}[G] = 0$, por cuanto $a \in A_i \Rightarrow aA_j = 0$ para todo $j \neq i$. Sin embargo, $ae = a \neq 0$. La contradicción obtenida muestra, que $\mathrm{Ker}\, \varphi = 0$. Por lo tanto, φ es un monomorfismo, y, como $\dim A_i = n_i^2 = \dim M_{n_i}(\mathbf{C})$, entonces, $A_i \overset{\varphi}{\cong} M_{n_i}(\mathbf{C})$. Tomando en cuenta la proposición 2, llegamos al teorema siguiente sobre la conformación del álgebra $\mathbf{C}[G]$.

TEOREMA 3. *El álgebra grupal* $\mathbf{C}[G]$ *del grupo finito* G *sobre el campo de los números complejos* $\mathbf{C}$ *se descompone en una suma directa* (2) *de ideales simples por ambos lados, isomorfos a las álgebras matriciales completas*:

$$\mathbf{C}[G] \oplus M_{n_1}(\mathbf{C}) \oplus M_{n_2}(\mathbf{C}) \oplus \ldots \oplus M_{n_r}(\mathbf{C}).$$

En particular, el álgebra grupal de un grupo abeliano de orden n sobre $\mathbf{C}$ *es isomorfa a la suma directa de r ejemplares del campo* $\mathbf{C}$. ∎

COROLARIO. (teorema de Bernsaid). *Sea* Φ *una representación matricial irreducible de grado n sobre* $\mathbf{C}$, *del grupo finito G. Entonces, entre las matrices* Φ_g, $g \in G$, *se tienen* n^2 *linealmente independientes, o sea,* $\langle \Phi_g \mid g \in G \rangle_{\mathbf{C}} = M_n(\mathbf{C})$. ∎

La conformación del centro $Z(\mathbf{C}[G])$ como una subálgebra conmutativa en $\mathbf{C}[G]$ se determina totalmente con las *constantes estruc-*

turales, que son los números enteros n_{ij}^k de las relaciones

$$z_i z_j = \sum_{k=1}^{r} n_{ij}^k z_k. \tag{4}$$

Teniendo en cuenta la expresión (3) para las z_i, es fácil comprender, que n_{ij}^k es el número de pares (g, h), $g \in g_i^G$, $h \in g_j^G$, para los cuales $gh = g_k$.

Tomemos en Z (C) $[G]$) otra base

$$e_i = \frac{n_i}{|G|} \sum_{k=1}^{r} \overline{\chi_i(g_k)}\, z_k = \frac{n_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)}\, g, \quad 1 \leqslant i \leqslant r. \tag{5}$$

Aquí, al igual que en el § 5, cap. 8, $\chi_1, \ldots, \chi_r$ son los caracteres de las representaciones irreducibles; $n_1, \ldots, n_r$, sus grados. El paso contrario se realiza por la fórmula

$$z_k = |g_k^G| \sum_{i=1}^{r} \frac{\chi_i(g_k)}{n_i} e_i.$$

Para convencerse de esto, es necesario utilizar la relación (4), § 5, cap. 8. Esta relación muestra, que

$$\sum_{i=1}^{r} e_i = \frac{1}{|G|} \sum_{g \in G} g \sum_i n_i \overline{\chi_i(g)} = \frac{1}{|G|} \sum_{g \in G} g \sum \chi_i(e) \overline{\chi_i(g)} =$$

$$= \frac{1}{|G|} e\, |C_G(e)| = e$$

Luego, empleando la relación generalizada de ortogonalidad del ejercicio 1, § 4, cap. 8, hallamos

$$e_i e_j = \frac{n_i n_j}{|G|^2} \sum_{g,\, t \in G} \overline{\chi_i(g)}\, \chi_j(t)\, gt =$$

$$= \frac{n_i n_j}{|G|^2} \sum_{h \in G} \left\{ \frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)}\, \chi_j(hg) \right\} h^{-1} =$$

$$= \frac{n_i n_j}{|G|} \frac{\delta_{ij}}{n_i} \sum \chi_i(h)\, h^{-1} = \delta_{ij} e_i.$$

De este modo, los elementos centrales e_i, calculados por la fórmula (5), satisfacen las relaciones

$$e = e_1 + e_2 \ldots + e_r, \qquad e_i^2 = e_i, \quad e_i e_j = 0, \quad i \neq j, \tag{6}$$

y se llaman, por esta razón (y por tradición), *idempotentes ortogonales centrales* del álgebra grupal C $[G]$. La relación $e = e_1 + \ldots + e_r$ es la condición para que este sistema resulte completo.

Haciendo $B_i = e_i \mathbf{C}[G]$, revelamos inmediatamente, que B_i es un ideal por ambos lados en $\mathbf{C}[G]$ con elemento unidad e_i, y que tiene lugar la descomposición en la suma directa

$$\mathbf{C}[G] = B_1 \oplus B_2 \oplus \ldots \oplus B_r. \tag{7}$$

De (5) se deduce inmediatamente, que

$$\chi_j(e_i) = n_i \frac{1}{|G|} \sum_g \overline{\chi_i(g)}\, \chi_j(g) = n_i \delta_{ij}.$$

Por eso, B_i contiene el ideal mínimo por la izquierda $J \subset A_i$, que responde al carácter χ_i. Como A_i y B_i son ideales por ambos lados, entonces, $A_i \subset B_i$. Comparando las descomposiciones (2) y (7), concluimos, que $A_i = B_i$. Y bien, ha quedado demostrada una variante más perfecta del teorema 3.

TEOREMA 4. *Los elementos e_i, $1 \leqslant i \leqslant r$, calculados según la fórmula* (5), *generan un sistema completo de idempotentes ortogonales centrales del álgebra grupal $\mathbf{C}[G]$ del grupo finito G. El componente primo $e_i\mathbf{C}[G]$ de la descomposición directa*

$$\mathbf{C}[G] = e_1\mathbf{C}[G] \oplus e_2\mathbf{C}[G] \oplus \ldots \oplus e_r\mathbf{C}[G],$$

es isomorfo al álgebra matricial completa $M_{n_i}(\mathbf{C})$, y contiene todos los ideales mínimos por la izquierda, que responden al carácter χ_i. ∎

Toda la teoría de representaciones de grupos se puede desarrollar a partir del teorema de Vedderbarn-Artin (véase el p. 1) y de la teoría estructural general de las álgebras grupales (su conclusión final para los grupos finitos se formuló en el teorema 3). Hemos ido en sentido opuesto, apoyándonos, en esencia, sólo en el lema de Schur.

Por último, demostremos una afirmación útil sobre los grados de las representaciones.

TEOREMA 5. *El grado n de la representación irreducible (Φ, V) sobre $\mathbf{C}$ del grupo finito G, divide el orden $|G|$.*

DEMOSTRACION. Sea $\widetilde{\Phi}$ la representación correspondiente al álgebra grupal $\mathbf{C}[G]$. Según el lema de Schur (proposición 3, § 3), el operador lineal $\widetilde{\Phi}(z_i)$ es permutable con todos los $\Phi(g)$, $g \in G$, y, por eso, pertenece a $\mathrm{End}_{\mathbf{C}[G]}(V)$, y debe ser múltiplo del operador unidad: $\widetilde{\Phi}(z_i) = w_i \mathcal{E}$. Tenemos

$$n\omega_i = \mathrm{tr}\, \omega_i \mathcal{E} = \mathrm{tr}\, \widetilde{\Phi}(z_i) = \sum \mathrm{tr}\, \Phi(g_i^h) = |g_i^G|\, \chi_\Phi(g_i),$$

de donde

$$\omega_i = \frac{|g_i^G|\, \chi_\Phi(g_i)}{n}.$$

Empleando $\tilde{\Phi}$ en las relaciones (4), obtenemos,

$$\omega_i \omega_j = \sum_{k=1}^{r} n_{ij}^k \omega_k.$$

Por lo tanto, $\mathbb{Z}[\omega_i]$ es submódulo del $\mathbb{Z}$ - módulo $\mathbb{Z}[\omega_1, \ldots, \omega_r]$ de tipo finito y, de acuerdo con los resultados del punto 3, § 3, ω_i es un número algebraico entero. Según los mismos resultados

$$\frac{|G|}{n} = \frac{|G|}{n} (\chi_\Phi, \chi_\Phi)_G = \frac{1}{n} \sum \chi_\Phi(g) \overline{\chi_\Phi(g)} =$$

$$= \frac{1}{n} \sum_{i=1}^{r} |g_i^G| \cdot \chi_\Phi(g_i) \overline{\chi_\Phi(g_i)} = \sum \omega_i \overline{\chi_\Phi(g_i)}$$

es un número algebraico entero. En consecuencia, $\frac{|G|}{n} \in \mathbb{Z}$. ∎

4. Algebras no asociativas. Sea A un álgebra cualquiera (o sea, no necesariamente asociativa) de dimensión arbitraria sobre el campo P. A cada tres elementos $x, y, z \in A$ les ponemos en correspondencia la expresión $(x, y, z) = (xy) z - x (yz)$ denominada *asociador* de los mismos. En dependencia de las relaciones idénticas, que vinculan a los asociadores o a otras expresiones, se obtienen distintos tipos (o, como también se dice, *clases primitivas*, *diversidades*) de álgebras. Sirven de ejemplos

1) *las álgebras asociativas*: $(x, y, z) = 0$;
2) *las álgebras elásticas*: $(x, y, x) = 0$;
3) *las álgebras alternativas*: $(x, x, y) = (y, x, x) = 0$;
4) *las álgebras de Jordan*: $(x, y, x^2) = 0$; $xy - yx = 0$.

Por este camino axiomático es posible, evidentemente, andar ilimitadamente. Es notable, sin embargo, que muchas clases de álgebras no asociativas aparecieron de un modo natural en ramas lejanas del álgebra como ciencia. En calidad de ejemplos más ilustrativos corresponde nombrar las álgebras de Jordan que llegaron a las matemáticas de la mecánica cuántica (de la física de Jordan), y las álgebras de Lie, utilizadas incialmente en forma exclusiva para la descripción (en determinadas condiciones) de la estructura local de los grupos topológicos (Sofus Lie, matemático del siglo XIX). Sobre las álgebras de Lie se hicieron menciones breves en las páginas del libro, por eso a ellas les destinamos un lugar aparte.

En el álgebra de Lie L sobre el campo P, el producto de los elementos $x, y \in L$ se acostumbra anotarlo $[xy]$. Por definición de las álgebras de Lie, la operación bilineal $(x, y) \mapsto [xy]$ satisface dos condiciones:

(i) $[xx] = 0$ ($[xy] = -[yx]$ *es anticonmutatividad*);
(ii) $[[xy] z] + [[yz] x] + [[zx] y] = 0$ (*identidad de Jacobi*).

EJEMPLO 1. Sea A un álgebra asociativa sobre el campo P. En el campo vectorial A damos una estructura de álgebra de Lie $L(A)$, haciendo $[xy] = xy - yx$. Es claro, que $[xx] = 0$. Luego,

$$[[xy]z] = (xy - yx)z - z(xy - yx) = xyz - yxz - zxy + zyx,$$
$$[[yz]x] = (yz - zy)x - x(yz - zy) = yzx - zyx - xyz + xzy,$$
$$[[zx]y] = (zx - xz)y - y(zx - xz) = zxy - xzy - yzx + yxz,$$

como resultado de una suma sencilla obtenemos la identidad de Jacobi.

Sea, en particular, $A = \mathrm{End}_P(V) = \mathfrak{L}(V)$, el álgabra de todos los operadores lineales del espacio vectorial finitodimensional V sobre P. Cualquier homomorfismo φ: $L \to L(\mathfrak{L}(V))$ se llama *representación del álgebra de Lie L*. El espacio de representaciones V también se denomina *L-módulo* (o *módulo sobre el álgebra de Lie L*). Formalmente, el L-módulo se da mediante tres axiomas:

$$\text{(L1)} \quad x(\alpha u + \beta v) = \alpha xu + \beta xv;$$
$$\text{(L2)} \quad (\alpha x + \beta y)v = \alpha xv + \beta yv;$$
$$\text{(L3)} \quad [xy]v = x(yv) - y(xv).$$

EJEMPLO 2. Se llama *diferenciación del álgebra* arbitraria K (no necesariamente asociativa) sobre el campo P, la diferenciación $\mathcal{D}$ del anillo K (véase la definición en el p. 3, § 1, cap. 6) permutable con la operación de una constante de P: $\mathcal{D}(\lambda a) = \lambda\mathcal{D}(a)$, $\lambda \in P$, $a \in K$. El ejemplo 1 y el ejercicio 8, § 1, cap. 6 muestran, que la multiplicación $[\mathcal{D}_1\mathcal{D}_2] = \mathcal{D}_1\mathcal{D}_2 - \mathcal{D}_2\mathcal{D}_1$ proporciona al conjunto Der (K), que es un espacio vectorial sobre P, estructura de álgebra de Lie. Si, en particular, $K = P[X]$ es un álgebra de los polinomios, entonces, Der (K) está compuesto de las diferenciaciones $\mathcal{D}_u$, $u \in K$ que operan de acuerdo con la regla: $\mathcal{D}_u(f) = u\dfrac{df}{dX} = uf'$. Por definición: $[\mathcal{D}_u\mathcal{D}_v](f) = \mathcal{D}_u(\mathcal{D}_v f) - \mathcal{D}_v(\mathcal{D}_u f) = \mathcal{D}_u(vf') - \mathcal{D}_v(uf') = u(vf')' - v(uf')' = u(v'f + vf'') - v(u'f' + uf'') = (uv' - u'v)f'$. Por consiguiente, $[\mathcal{D}_u\mathcal{D}_v] = \mathcal{D}_{uv'-u'v}$ y vemos, que el álgebra Der (K) es isomorfa al álgebra infinitadimensional de Lie $(K, [\ ])$ con el espacio base K y la multiplicación $[uv] = uv' - u'v$. Haciendo $K_{(i)} = (X^{i+1})\mathbb{C}$, obtenemos la descomposición de K en la suma directa

$$K = K_{(-1)} \oplus K_{(0)} + K_{(1)} \oplus K_{(2)} \oplus \ldots,$$

que tiene la propiedad del *álgebra graduada de Lie*: $[K_{(i)}K_{(j)}] \supset K_{(i+j)}$ (comparar con el ejemplo 2 del punto 1). E álbebra de Lie $(K, [\ ])$ opera en el espacio vectorial K de dos maneras: 1) $(a, f) \mapsto af'$ (*operación natural*); 2) $(a, f) \mapsto af' - a'f$ (*operación con endomorfismos adjuntos*). Como resultado, se obtienen dos $(K, [\ ])$-módulos no isomorfos.

EJEMPLO 3. Las matrices antisimétricas con traza nula K_1, K_2, K_3, construidas en el ejercicio 3, § 1, cap. 7, respecto al grupo SU (2), satisfacen las relaciones

$$[K_1K_2] = K_3, \quad [K_2K_3] = K_1 \; [K_3K_1] = K_2,$$

que repiten con exactitud la regla del producto vectorial de vectores en $\mathbb{R}^3$ ($[K_sK_t] = K_sK_t - K_tK_s$ que son «conmutadores» de las matrices en $M_2(\mathbb{C})$; véase el ejemplo 1). Por eso, el espacio real tridimensional $\langle K_1, K_2, K_3\rangle_\mathbb{R}$ está dotado de la estructura del álgebra de Lie.

De la teoría general de representaciones de grupos compactos se deduce, que entre las representaciones irreducibles del grupo SU (2) y sus álgebras de Lie su (2) $= \langle K_1, K_2, K_3\rangle_\mathbb{R}$ se tiene correspondencia biunívoca. Esto se puede comprender intuitivamente, tomando en

cuenta la continuidad de la representación del grupo y examinando en la envoltura lineal de los operadores $\Phi(g_t)$ (donde g_t es un elemento dependiente de un modo diferenciable del $t \in R$ del grupo SU (2); $g_0 = e$) el operador lineal $\lim_{t \to 0} \frac{1}{t} \Phi(g_t)$, ya contenido en el álgebra su (2). A fin de confirmar el listado completo de las representaciones irreducibles del grupo SU (2), que fueron obtenidas en el § 6, cap. 8, nos es necesario convencernos de que, para cualquier n natural se tiene, con exactitud hasta el isomorfismo, exactamente un su (2)-módulo irreducible de dimensión n sobre C. Con este fin, es cómodo pasar desde el principio del álgebra real de Lie su (2) a su «complejificación», que coincide con el álgebra de Lie

$$L = \mathrm{sl}\,(2) = \mathrm{su}\,(2) \otimes_R C$$

de todas las 2 × 2-matrices complejas con traza nula. Los elementos básicos

$$e_{-1} = -iK_1 + K_2, \quad e_0 = -2iK_3, \quad e_1 = -iK_1 - K_2$$

del álgebra L se multiplican de acuerdo con la regla

$$[e_{-1}e_1] = e_0, \quad [e_0e_{-1}] = -2e_{-1}, [e_0e_1] = 2e_1. \qquad (8)$$

Olvidando por un momento el origen de L, puede considerarse, que $L = \langle e_{-1}, e_0, e_1 \rangle C$ es un álgebra tridimensional abstracta de Lie sobre C con tabla de multiplicación (8). Es fácil comprobar que L es un álgebra prima de Lie. Por lo tanto, cualquier módulo irreducible suyo de dimensión >1, será exacto.

Sea, inicialmente, $V \neq 0$, un L-módulo arbitrario de dimensión finita sobre C, y sean, E_{-1}, E_0, E_1, operadores lineales en V, propiamente correspondientes a los elementos e_{-1}, e_0, e_1. En la teoría de las representaciones de las álgebras de Lie, se ha establecido su propia terminología, que observaremos. El subespacio propio $V^\lambda = \{v \in V \mid E_0v = \lambda v\}$ del operador E_0 en V con el valor propio $\lambda \in C$ está compuesto por vectores, sobre los cuales es aceptado decir, que tienen un *peso* λ. La dimensión $\dim V^\lambda$ se llama *multiplicidad del peso* λ.

LEMA 1. *Si* $v \in V^\lambda$, entonces, $E_1v \in V^{\lambda+2}$, $E_{-1}v \in V^{\lambda-2}$ (E_1 es *operador «aumentativo», y* E_{-1} *«diminutivo»*).

DEMOSTRACION. En concordancia con el axioma (L3) tenemos $E_0(E_1v) = [E_0E_1]\,v + E_1(E_0v) = 2E_1v + E_1(\lambda v) = (\lambda + 2)\,E_1v$, así que, por definición, $E_1v \in V^{\lambda+2}$. Análogamente, $E_0(E_{-1}v) = (\lambda - 2)\,E_{-1}v$.

Del curso del álgebra lineal se sabe, que los vectores que responden a distintos valores propios, son linealmente independientes. Por eso, la suma $W = \sum_\lambda V^\lambda \subset V$ es directa. Del lema 1, también se deduce, que $W = \sum_\lambda V^\lambda$ es L-submódulo en V. Como $W \neq 0$, enton-

ces, en caso de un L-módulo irreducible V, debe cumplirse la igualdad $W = V$.

Llamemos al vector $v_0 \in V$ *vector mayor de peso* λ, si $v_0 \neq 0$ y $E_1 v_0 = 0$, $E_0 v_0 = \lambda v_0$.

LEMA 2. *Cualquier L-módulo V finitodimensional, tiene vector mayor.*

DEMOSTRACION. Tomemos un vector v arbitrario ($\neq 0$) de peso μ y compongamos la sucesión de vectores $v, E_1 v, E_1^2 v, \ldots$, con pesos μ, $\mu + 2$, $\mu + 4, \ldots$ (véase el lema 1). Como $\dim V < \infty$, entonces, $E_1^{m+1} v = 0$ para algún m. Tomando m el mínimo, podemos hacer $v_0 = E_1^m v$, $\lambda = \mu + 2m$.

En calidad de ejemplo examinemos el espacio vectorial V_n de dimensión $n + 1$ sobre $\mathbf{C}$ con base fijada $v_0, v_1, \ldots, v_n$. Los operadores E_{-1}, E_0, E_1, los determinamos mediante las fórmulas

$$\begin{aligned} E_{-1} v_m &= (m + 1)\ v_{m+1}, \\ E_0 v_m &= (n - 2m)\ v_m, \\ E_1 v_m &= (n - m + 1)\ v_{m-1}, \end{aligned} \tag{9}$$

haciendo $v_{-1} = 0 = v_{n+1}$. La comprobación directa muestra, que se han cumplido las relaciones

$$\begin{aligned} E_1\ (E_{-1} v_m) - E_{-1}(E_1 v_m) &= E_0 v_m, \\ E_0\ (E_{-1} v_m) - E_{-1}\ (E_0 v_m) &= -2E_{-1} v_m, \\ E_0\ (E_1 v_m) - E_1\ (E_0 v_m) &= 2E_1 v_m, \end{aligned}$$

que están en correspondencia con la tabla de multiplicación (8) y con los axiomas del L-módulo. Como $E_1 v_0 = (n + 1)\ v_{-1} = 0$, $E_0 v_0 = n v_0$, entonces, v_0 es el vector de peso n, y todo el espacio V_n se escribe en forma de la suma directa

$$V_n = V^n \oplus V^{n-2} \oplus \ldots \oplus V^{-n} \tag{10}$$

de espacios unidimensionales de «pesos» $V^{n-2m} = \langle v_m \rangle$ (cada peso tiene la multiplicidad 1). Suponiendo la existencia del submódulo $U \neq 0$ en V_n, tomamos cualquier vector propio $u \in U$ del operador E_0. De acuerdo con la descomposición (10), $u = \lambda v_m$ para algún m. El empleo sucesivo del operador «aumentativo» E_1 (véase la fórmula (9)) nos da las inclusiones $v_{m-1} \in U, \ldots, v_0 \in U$, y mediante el operador «disminutivo» E_{-1} obtenemos del vector mayor v_0 los restantes vectores. Por lo tanto, $U = V_n$ y V_n es un L-módulo irreducible.

Observemos, que V_0 es un módulo trivial (unidimensional), y V_1 es el módulo correspondiente a la definición natural del álgebra L: en la base $\{v_0, v_1\}$ los operadores E_{-1}, E_0, E_1, tienen como sus matrices

$$\begin{Vmatrix} 0 & 0 \\ 1 & 0 \end{Vmatrix}, \quad \begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}, \quad \begin{Vmatrix} 0 & 1 \\ 0 & 0 \end{Vmatrix}.$$

El teorema siguiente resuelve el problema que nos ocupa.

TEOREMA 6. *Todo L-módulo V irreducible de dimensión n+ 1 sobre* $\mathbb{C}$ *es isomorfo a* V_n.

DEMOSTRACION. Según el lema 2, nuestro módulo V posee cierto vector mayor v_0 de peso λ. Hagamos $v_{-1} = 0$ y $v_m = \frac{1}{m!} E_{-1}^m v_0 = \frac{1}{m!} E_{-1} (\ldots (E_{-1} v) \ldots)$ para $m \geqslant 0$. Se afirma, que para cualquier $m \geqslant 0$ son legítimas las fórmulas

$$\begin{aligned} E_{-1} v_m &= (m+1)\ v_{m+1}, \\ E_0 v_m &= (\lambda - 2m)\ v_m, \\ E_1 v_m &= (\lambda - m + 1)\ v_{m-1}. \end{aligned} \tag{10}$$

Efectivamente, cuando $m = 0$, las fórmulas (10′) se reducen a la determinación del vector mayor v_0 y del vector v_1, a continuación, operamos por inducción respecto a m: a) por la fórmula $E_{-1} v_m = (m+1)\ v_{m+1}$ se determina el vector v_{m+1}; b) la formula $E_0 v_m = (\lambda - 2m)\ v_m$ se deduce del lema 1; c) si ya se sabe, que $E_1 v_{m-1} = (\lambda - m + 2)\ v_{m-2}$, entonces después de simplificar por m ambas partes de la igualdad

$$\begin{aligned} mE_1 v_m &= E_1(E_{-1} v_{m-1}) = [E_1 E_{-1}]\ v_{m-1} + E_{-1}\ (E_1 v_{m-1}) = \\ &= E_0 v_{m-1} + (\lambda - m + 2)\ E_{-1} v_{m-2} = \\ &= \{(\lambda - 2m + 2) + (\lambda - m + 2)\ (m-1)\}\ v_{m-1} = \\ &= m\ (\lambda - m + 1)\ v_{m-1} \end{aligned}$$

se obtiene la última de las fórmulas (10′).

Si los vectores $v_0, v_1, \ldots, v_r$, para algún r son diferentes de cero, entonces, teniendo distintos pesos, ellos deben ser linealmente independientes. Por otro lado, en virtud de la irreducibilidad de V, el submódulo, engendrado por el vector v_0, coincide con V, y, como $\dim V = n + 1$, entonces, $V = \langle v_0, v_1, \ldots, v_n \rangle$ y $v_{n+1} = v_{n+2} = \ldots = 0$. En particular,

$$0 = E_1 v_{n+1} = (\lambda - n)\ v_n = 0 \Rightarrow \lambda = n$$

(prestemos atención a la curiosa implicación $\dim V < \infty \Rightarrow \lambda \in \mathbb{Z}$, $\lambda \geqslant 0$).

Sustituyendo el valor $\lambda = n$ en las fórmulas (10′), de hecho llegamos, tomando en cuenta las designaciones elegidas, a las fórmulas (9), mediante las que se determina el L-módulo V_n. En consecuencia, $V \cong V_n$.

EJERCICIOS

1. ¿Cuántas resoluciones en el álgebra de los cuaterniones $\mathbb{H}$ tiene la ecuación $x^2 + 1 = 0$?

2. *Algebra de cuaterniones generalizados sobre* $\mathbb{Q}$. Mostrar, que con la tabla de multiplicación

	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	n	e_3	ne_2
e_2	e_2	$-e_3$	m	$-me_1$
e_3	e_3	$-ne_2$	me_1	$-nm$

con $n, m \in \mathbb{Z}$, $nm \neq 0$, en el espacio vectorial tetradimensional $\mathbb{H}(n, m) = \langle 1, e_1, e_2, e_3\rangle_Q$ sobre Q, se introduce la estructura del álgebra asociativa con unidad. Utilizar para este fin la representación

$$x = x_0 + x_1e_1 + x_2e_2 + x_3e_3 \mapsto A_x = \begin{Vmatrix} x_0 + x_1\sqrt{n} & x_2\sqrt{m} + x_3\sqrt{nm} \\ x_2\sqrt{m} - x_3\sqrt{mn} & x_0 - x_1\sqrt{n} \end{Vmatrix}.$$

El determinante $\det A_x = x_0^2 - x_1^2n - x_2^2m + x_3^2nm = N(x)$ se llama norma del elemento x. Comprobar, que cuando se cumple la condición $x \in \mathbb{H}(n, m)$, $x \neq 0 \Rightarrow N(x) \neq 0$, el espacio $\mathbb{H}(n, m)$ es un álgebra con división (*álgebra generalizada de los cuaterniones*). Utilizando los conceptos y resultados del ejercicio 7, § 2, mostrar, que para $p = \pm 3 \pmod 8$ primo, el álgebra $\mathbb{H}(2, p)$ será álgebra con división.

3. Examinar $\mathbb{F}_{2^n}$ como espacio vectorial V de dimensión n sobre $\mathbb{F}_2$. Junto con la operación de suma, heredada de $\mathbb{F}_{2^n}$, introducir en V la operación de multiplicación $(x, y) \mapsto x \circ y = \sqrt{xy}$. Aquí, $x \mapsto \sqrt{x}$ es automorfismo en $\mathbb{F}_{2^n}$, inverso de $x \mapsto x^2$, así que $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$. Mostrar que $(V, +, \circ)$ es un álgebra conmutativa (no asociativa) sobre $\mathbb{F}_2$, poseedora de las propiedades: a) en V no hay divisores de cero ni unidad; b) la ecuación $a \circ x = b$ con $a \neq 0$ se resuelve unívocamente; c) el grupo de los automorfismos $\mathrm{Aut}(V)$ opera en $V \setminus \{0\}$ transitivamente.

4. En cualquier álgebra se cumple la identidad

$$t(x, y, z) + (t, x, y)z = (tx, y, z) - (t, xy, z) + (t, x, yz).$$

Convencerse de esto mediante la comprobación y mostrar, que si el álgebra A con unidad 1 sobre el campo P para todos los asociadores tiene lugar la inclusión $(x, y, z) \in P\cdot 1$, entonces, A es un álgebra asociativa.

Complemento

FORMA NORMAL DE JORDAN DE MATRICES

Esta «isla» del álgebra lineal se trata brevemente aquí, sólo para subrayar su parecido con el § 5, cap. 7, donde se da la clasificación de los grupos abelianos finitos. No consideramos necesario insistir, en el § 3, cap. 9, en el papel asociativo que desempeñan en esta cuestión los módulos sobre anillos de ideales principales, por cuanto para distintas categorías de lectores, posiblemente, será más cómodo tener demostraciones directas de los hechos correspondientes sobre los grupos y acerca de los operadores lineales.

1. Tratando de interpretar la operación del operador lineal dado $\mathcal{A}\colon V \to V$, es natural proponerse como meta el hallar la base en V, que concuerde del mejor modo con $\mathcal{A}$. Con otras palabras, en la clase de matrices semejantes $C^{-1}AC$, que responden al operador $\mathcal{A}$, se requiere hallar la matriz que tenga la forma más sencilla posible. Por razones comprensibles, esta tarea está esencialmente ligada con el campo básico P, sobre el cual está definido el espacio vectorial V. En adelante, consideraremos que $P = \mathbb{C}$ es el campo de los números complejos o cualquier campo algebraicamente cerrado.

Sea $n = \dim V$ y $\lambda_1, \ldots, \lambda_n$, las raíces características del polinomio

$$f_{\mathcal{A}}(t) = f_A(t) = \det(tE - A) = t^n + a_1 t^{n-1} + \ldots + a_n = \prod_{i=1}^{n} (t - \lambda_i),$$

$$a_1 = -\operatorname{tr} A = -(\lambda_1 + \ldots + \lambda_n),$$
$$a_n = (-1)^n \det A = (-1)^n \lambda_1 \ldots \lambda_n.$$

Los números complejos λ_i son también valores propios del operador lineal $\mathcal{A}$: los subespacios

$$V^{\lambda_i} = \{v \in V \mid \mathcal{A}v = \lambda_i v\}$$

diferentes de cero y sus vectores no nulos se llaman vectores propios del operador $\mathcal{A}$. El conjunto Spec $(\mathcal{A})$ de todos los distintos valores propios (raíces características) de dos en dos del operador $\mathcal{A}$ se llama *espectro* del operador $\mathcal{A}$. Análogamente se dice sobre el *espectro* Spec (A) *de la matriz* A.

Señalemos los hechos siguientes:

(i) *Los vectores propios, pertenecientes a distintos valores propios, son linealmente independientes. La suma* $\sum_{\lambda \in \mathrm{Spec}(A)} V^{\lambda}$ *es directa* (hablando en general, $\sum V^{\lambda}$ no coincide con V).

(ii) *La matriz del operador lineal* $\mathcal{A}$ *siempre puede ser reducida (en el sentido de semejanza) a la forma triangular.*

La forma más fácil de convencerse de esto es razonando por inducción. Es necesario tomar un subespacio $\langle e_1 \rangle$ ($\mathcal{A}e_1 = \lambda_1 e_1$), $\mathcal{A}$-invariable unidimensional, pasar al espacio cociente $\overline{V} = V/\langle e_1 \rangle = \{\overline{v} = v + \langle e_1 \rangle \mid v \in V\}$ de dimonsión $n - 1$ y al operador cociente $\overline{\mathcal{A}}$: $\overline{\mathcal{A}}\,\overline{v} = \overline{\mathcal{A}v}$, elegir en $\overline{V}$ la base $\overline{e}_2, \ldots, \overline{e}_n$, que lleva a $\overline{A}$ la forma triangular, y regresar al espacio V:

$$A = \begin{Vmatrix} \lambda_1 & & & * \\ & \lambda_2 & & \\ 0 & & \ddots & \\ & & & \lambda_n \end{Vmatrix}. \quad \blacksquare$$

(iii) (Teorema de Hamilton—Cayley). *El operador lineal $\mathcal{A}$ y su matriz correspondiente A (en cualquier base) se anulan con su polinomio característico.*

Como esta afirmación no depende de la elección de la base, entonces, resulta cómodo usar la propiedad (ii). Examinemos la cadena de subespacios *$\mathcal{A}$-invariantes* $V = V_0 \supset V_1 \supset \ldots \supset V_{n-1} \supset 0$, donde $V_k = \langle e_1, e_2, \ldots, e_{n-k-1}, e_{n-k} \rangle$. Como $(\mathcal{A} - \lambda_{n-k}\mathcal{E})\, e_{n-k} \in V_{k+1}$, entonces, $(\mathcal{A} - \lambda_{n-k}\mathcal{E})\, V_k \subset V_{k+1}$ y, por lo tanto,

$$f_{\mathcal{A}}(\mathcal{A})V = \prod_{i=1}^{n} (\mathcal{A} - \lambda_i \mathcal{E})V =$$
$$= (\mathcal{A} - \lambda_1\mathcal{E}) \ldots (\mathcal{A} - \lambda_n\mathcal{E}) V_0 \subset (\mathcal{A} - \lambda_1\mathcal{E}) \ldots (\mathcal{A} - \lambda_{n-1}\mathcal{E}) V_1 \subset$$
$$\subset (\mathcal{A} - \lambda_1\mathcal{E}) \ldots (\mathcal{A} - \lambda_{n-2}\mathcal{E}) V_2 \subset \ldots \subset (\mathcal{A} - \lambda_1\mathcal{E}) V_{n-1} = 0.$$

Pero $f_{\mathcal{A}}(\mathcal{A})V = 0 \Leftrightarrow f_{\mathcal{A}}(\mathcal{A}) = 0$. $\blacksquare$

(iv) *El polinomio mínimo $h_{\mathcal{A}}(t) = h_A(t)$ del operador (polinomio unitario de grado mínimo $m \leqslant n$, anulador de $\mathcal{A}$ y A) es divisor del polinomio característico $f_{\mathcal{A}}(t)$, divisible por todos los multiplicadores lineales $t - \lambda$, $\lambda \in$ Spec $(\mathcal{A})$.*

La división con resto $f_{\mathcal{A}}(t) = q(t) \cdot h_{\mathcal{A}}(t) + r(t)$, $\deg r(t) < \deg h_{\mathcal{A}}(t)$, y las propiedades $f_{\mathcal{A}}(\mathcal{A}) = 0 = h_{\mathcal{A}}(\mathcal{A})$ muestran, que $r(\mathcal{A}) = 0$, de donde $r(t) = 0$. Si, luego, λ es el valor propio del operador $\mathcal{A}$, entonces, $\mathcal{A}v = \lambda v \Rightarrow 0 = h_{\mathcal{A}}(\mathcal{A})\, v = h_{\mathcal{A}}(\lambda)v \Rightarrow h_{\mathcal{A}}(\lambda) = 0 \Rightarrow (t - \lambda) \mid h_{\mathcal{A}}(t)$.

EJEMPLO. El operador lineal $\mathcal{A}$: $V \to V$ se llama *nilpotente*, si $\mathcal{A}^m = 0$; m es el *índice de nilpotencia*, si $\mathcal{A}^{m-1} \neq 0$. *Sea $\mathcal{A}^{m-1}v \neq 0$. Entonces, los vectores $v, \mathcal{A}v, \ldots, \mathcal{A}^{m-1}v$, son linealmente independientes.* En efecto, toda dependencia lineal no trivial tiene la forma

$$\mathcal{A}^k v + \alpha_1 \mathcal{A}^{k+1} v + \ldots + \alpha_{m-1-k} \mathcal{A}^{m-1} v = 0, \quad 0 \leqslant k \leqslant m - 1.$$

La aplicación del operador $\mathcal{A}^{m-1-k}$ a ambos miembros de esta igualdad nos llevaría a la relación $\mathcal{A}^{m-1}v = 0$, lo que contradice la elección de v.

Y bien, el índice de nilpotencia m del operador $\mathcal{A}$ no supera $n = \dim V$. Sean, $m = n$ y $\mathcal{A}^{n-1}e \neq 0$. Introduzcamos las designaciones siguientes para

los vectores básicos: $e_1 = \mathcal{A}^{n-1}e$, $e_2 = \mathcal{A}^{n-2}e$, . . ., $e_{n-1} = \mathcal{A}e$, $e_n = e$. Entonces, $\mathcal{A}e_1 = 0$, $\mathcal{A}e_k = e_{k-1}$, $k > 1$, y la matriz del operador $\mathcal{A}$ en la base $\{e_1, \ldots, e_n\}$ será la célula de Jordan

$$J_{n,0} = \begin{Vmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{Vmatrix}$$

Si, por ejemplo, $V = \langle 1, X, X^2, \ldots, X^{n-1} \rangle_{\mathbb{C}}$ es el espacio de los polinomios de grado $< n$ sobre $\mathbb{C}$, y $\mathcal{A} = \frac{d}{dX}$ es el operador de diferenciación, entonces, la matriz de este operador en la base $\{e_i\}$, $e_i = \frac{1}{i!} X^i$ será, precisamente, la célula $J_{n,0}$.

Más generalmente, llamemos *célula* (*superior*) *de Jordan* de dimensión $m \times m$ (o de orden m), correspondiente al valor propio de λ, a la matriz

$$J_{m,\lambda} = \begin{Vmatrix} \lambda & 1 & 0 & \ldots & 0 & 0 \\ 0 & \lambda & 1 & \ldots & 0 & 0 \\ 0 & 0 & \lambda & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & \lambda & 1 \\ 0 & 0 & 0 & \ldots & 0 & \lambda \end{Vmatrix}.$$

Observemos, que $J_{m,\lambda} - \lambda E = J_{m,0}$ es la matriz nilpotente: $J_{m,0}^{m-1} \neq 0$, $J_{m,0}^{m} = 0$.

En particular, $(t - \lambda)^m$ es el polinomio mínimo de la célula de Jordan $J_{m,\lambda}$ y λ, su único valor propio: Spec $(J_{m,\lambda}) = \{\lambda\}$.

Si $u(t)$ es un polinomio arbitrario, entonces

$$u(J_{m,\lambda}) = \begin{Vmatrix} u(\lambda) & u'(\lambda)/1! & u''(\lambda)/2! & \ldots & u^{(m-1)}(\lambda)/(m-1)! \\ 0 & u(\lambda) & u'(\lambda)/1! & \ldots & u^{(m-2)}(\lambda)/(m-2)! \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & u(\lambda) \end{Vmatrix},$$

así que es mucho más fácil operar con $J_{m,\lambda}$, que con matrices arbitrarias.

TEOREMA FUNDAMENTAL. *Cada matriz cuadrada A de orden n sobre el campo algebraico cerrado P (en particular, sobre $\mathbb{C}$) es semejante a la suma directa de las células de Jordan. Precisamente, existe una matriz*

no degenerada C, para la cual

$$C^{-1}AC = J_{m_1,\lambda_1} \dot{+} \ldots \dot{+} J_{m_s,\lambda_s} = \begin{Vmatrix} J_{m_1,\lambda_1} & & & \\ & J_{m_2,\lambda_2} & & 0 \\ & 0 & \ddots & \\ & & & J_{m_s,\lambda_s} \end{Vmatrix}$$

(*forma normal de Jordan* $J(A)$ *de la matriz* A). *Con exactitud hasta la permutación de las células, la forma normal de Jordan de la matriz es única.*

Como los polinomios mínimos de las matrices semejantes coinciden, entonces, del teorema fundamental y de las observaciones, hechas con respecto a la célula de Jordan $J_{m,\lambda}$, se deduce, que

$$h_A(t) = (t - \lambda_{i_1})^{m_{i_1}} \ldots (t - \lambda_{i_p})^{m_{i_p}},$$

donde $\{\lambda_{i_1}, \ldots, \lambda_{i_p}\} = \text{Spec}(A)$ y m_{j_k} es el orden máximo de la célula de Jordan, que responde al valor proprio de λ_{j_k}.

El claro, que la condición necesaria y suficiente de diagonalización de la matriz A (o sea, la semejanza de su matriz diag $\{\lambda_1, \ldots, \lambda_n\}$ es la ausencia en $J(A)$ de células de orden mayor de 1. Por, eso, se obtiene el siguiente criterio útil.

COROLARIO. La *matriz cuadrada* A *sobre* C *se diagonaliza si, y sólo si, su polinomio mínimo* $h_A(t)$ *no tiene raíces múltiples.*

Este criterio es efectivo, por cuanto para el cálculo de $h_A(t)$ no es necesario reducir la matriz A a la forma normal de Jordan.

La demostración del teorema fundamental se divide en tres partes, correspondientes a los puntos 2, 3, 4.

2. El conjunto de vectores

$$V(\lambda) = \{v \in V \mid (\mathcal{A} - \lambda\mathcal{E})^k v = 0 \text{ para algún } k\}$$

se llama *subespacio radical*, correspondiente al valor propio de $\lambda \in \in \text{Spec}(\mathcal{A})$.

De que $V(\lambda)$ es un subespacio, nos convence una comprobación fácil. Si, por ejemplo, $u \in V(\lambda)$, $v \in V(\lambda)$, siendo además, $(\mathcal{A} - \lambda\mathcal{E})^s u = 0$, $(A - \lambda\mathcal{E})^t v = 0$ y $m = \text{máx}\{s, t\}$, entonces,

$$(A - \lambda\mathcal{E})^m (\alpha u + \beta v) = \alpha (\mathcal{A} - \lambda\mathcal{E})^m u + \beta (\mathcal{A} - \lambda\mathcal{E})^m v = 0,$$

de donde $\alpha u + \beta v \in V(\lambda)$ para cualesquiera $\alpha, \beta \in C$. Como en $V(\lambda)$ está contenido el vector propio, correspondiente a λ, entonces, $V(\lambda) \neq 0$. Luego, $V^\lambda \subset V(\lambda)$, pero, la igualdad puede no existir, como lo demuestra el ejemplo del operador nilpotente $\mathcal{A}$ de índice de nilpotencia n. En este caso, $\lambda = 0$ es el único valor propio, $\dim V^0 = 1$, pero $V(0) = V$.

Como $\dim V(\lambda) \leqslant n$ y la limitación $\mathcal{A} - \lambda\mathcal{E}$ en $V(\lambda)$ es un operador nilpotente, entonces,

$$V(\lambda) = \{v \in V \mid (\mathcal{A} - \lambda\mathcal{E})^n v = 0\}.$$

TEOREMA 1. *Sea $\mathcal{A}$: $V \to V$, un operador lineal con polinomio característico*

$$f_{\mathcal{A}}(t) = \prod_{i=1}^{p} (t-\lambda_i)^{n_i} \quad (\lambda_i \neq \lambda_j \text{ para } i \neq j).$$

Entonces, $V = V(\lambda_1 \oplus \ldots \oplus V(\lambda_p)$ es la suma directa de los subespacios radicales $V(\lambda_i)$, cada uno de los cuales es invariante respecto a $\mathcal{A}$ y tiene la dimensión $\dim V(\lambda_i) = n_i$. El operador $\mathcal{A} - \lambda_i\mathcal{E}$, nilpotente en $V(\lambda_i)$, opera de un modo no degenerado en el subespacio

$$V_i = V(\lambda_1) \oplus \ldots \oplus V(\lambda_{i-1}) \oplus V(\lambda_{i+1}) \oplus \ldots \oplus V(\lambda_p).$$

Finalmente, λ_i es el único valor propio del operador $\mathcal{A} \mid V(\lambda_i)$.

DEMOSTRACION. Ninguno de los factores primos $t - \lambda_k$ puede ser, a un mismo tiempo, divisor de todos los polinomios

$$f_i(t) = \prod_{j \neq i} (t-\lambda_j)^{n_j}, \quad i = 1, 2, \ldots, p,$$

y, por eso, el m.c.d. $(f_1(t), \ldots, f_p(t)) = 1$. Existen, por lo tanto, polinomios $g_1(t), \ldots, g_p(t) \in \mathbb{C}[t]$, para los cuales

$$\sum_{i=1}^{p} f_i(t) g_i(t) = 1. \tag{1}$$

Los subespacios

$$W_i = f_i(\mathcal{A}) g_i(\mathcal{A}) V = \{f_i(\mathcal{A}) g_i(\mathcal{A}) v \mid v \in V\} \quad 1 \leqslant i \leqslant p,$$

son invariantes respecto a $\mathcal{A}$:

$$\mathcal{A} W_i = f_i(\mathcal{A}) g_i(\mathcal{A}) \mathcal{A} V \subset f_i(\mathcal{A}) g_i(\mathcal{A}) V = W_i.$$

Además,

$$(\mathcal{A} - \lambda_i \mathcal{E})^{n_i} W_i = f_{\mathcal{A}}(\mathcal{A}) g_i(\mathcal{A}) V = 0$$

(por cuanto $f_{\mathcal{A}}(\mathcal{A}) = 0$; véase (iii)), así que

$$W_i \subset V(\lambda_i). \tag{2}$$

La reelación (1), reescrita en la forma

$$\mathcal{E} = \sum_{i=1}^{p} f_i(\mathcal{A}) g_i(\mathcal{A}),$$

nos da la descomposición

$$V = \sum_{i=1}^{p} W_i$$

y además (en virtud de la inclusión (2)):

$$V = \sum_{i=1}^{p} V(\lambda_i).$$

Supongamos, que $v \in V(\lambda_i) \cap V_i$, donde, al igual que en la formulación del teorema $V_i = \sum_{j \neq i} V(\lambda_j)$. Entonces, $(\mathcal{A} - \lambda_i \mathcal{E})^n v = 0$, y, como $v = \sum_{j \neq i} v_j$ y $(\mathcal{A} - \lambda_j \mathcal{E})^n v_j = 0$, entonces, $\{\prod_{j \neq i} (\mathcal{A} - \lambda_j \mathcal{E})^n\} v = 0$. Pero, del hecho de que son primos entre sí los polinomios $(t - \lambda_i)^n$, $c(t) = \prod_{j \neq i} (t - \lambda_j)^n$, se deduce la existencia de $a(t)$, $b(t)$, para los cuales,

$$a(t)(t - \lambda_i)^n + b(t) c(t) = 1.$$

Obtenemos

$$v = a(\mathcal{A})(\mathcal{A} - \lambda_i)^n v + b(\mathcal{A}) \{\prod_{j \neq i} (\mathcal{A} - \lambda_j \mathcal{E})^n\} v = 0,$$

o sea, los espacios $V(\lambda_i)$ y V_i no se intersecan. En consecuencia, tenemos la descomposición

$$V = V(\lambda_1) \oplus \ldots \oplus V(\lambda_p) \tag{3}$$

en una suma directa de subespacios $\mathcal{A}$-invariantes.

De la inclusión (2) y de la descomposición (3) se deduce inmediatamente, que $W_i = V(\lambda_i)$. De este modo, para $V(\lambda_i)$ se ha obtenido la expresión efectiva

$$V(\lambda_i) = f_i(\mathcal{A}) g_i(\mathcal{A}) V,$$

donde $f_i(t)$, $g_i(t)$, son polinomios de la identidad (1). En particular,

$$(\mathcal{A} - \lambda_i)^{n_i} V(\lambda_i) = 0.$$

Algún divisor del polinomio $(t - \lambda_i)^{n_i}$ será polinomio mínimo para A en $V(\lambda_i)$. De esto se deduce, en primer lugar, que λ_i es el único valor propio del operador $\mathcal{A}|_{V(\lambda_i)}$. Luego, en la base que es la unión de las bases de los espacios $V(\lambda_i)$, el operador $\mathcal{A}$ tiene la matriz

$$A = \begin{Vmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_p \end{Vmatrix},$$

donde A_i es una matriz de orden $n_i' = \dim V(\lambda_i)$ con el valor propio único λ_i y el polinomio característico $f_{A_i}(t) = (t - \lambda_i)^{n_i'}$, $n_i' \leqslant \leqslant n_i$. Como $f_A(t) = \prod_{i=1}^{p} f_{A_i}(t)$, entonces, $n = n_1' + \ldots + n_p'$ y $n_i' = n_i$.

Nos queda por demostrar que la limitación $(\mathcal{A} - \lambda_i \mathcal{E})|_{V_i}$ es no degenerada. Pero esto es comprensible: en caso contrario, $\{\operatorname{Ker}(\mathcal{A} - \lambda_i \mathcal{E})\} \cap V_i \neq 0$ y $\mathcal{A}v - \lambda_i v = 0$ para algún $0 \neq v \in V_i$. Sin embargo, en V_i el polinomio característico para $\mathcal{A}$ resulta ser $f_i(t) = \prod_{j \neq i} (t - \lambda_j)^{n_j}$, y λ_i no puede ser valor propio.

3. La cuestión sobre la elección de la matriz más sencilla, demostrada en el teorema 1, para el operador lineal $\mathcal{A}: V \to V$, se llevó al caso cuando $\mathcal{A}$ tiene un valor propio único λ y $(\mathcal{A} - \lambda\mathcal{E})^m = 0$, $m \leqslant \dim V$. Haciendo $\mathcal{B} = A - \lambda\mathcal{E}$, obtenemos el operador nilpotente de índice de nilpotencia m con matriz nilpotente B.

TEOREMA 2. *La forma normal de Jordan $J(B)$ de la matriz nilpotente B, existe* (el campo básico P, es arbitrario).

DEMOSTRACIÓN. Nos es necesario demostrar, que el espacio vectorial V, en el cual opera el operador nilpotente $\mathcal{B}$ con la matriz B, se descompone en la suma directa de los llamados *subespacios cíclicos* $P[\mathcal{B}]v_i = \langle v_i, \mathcal{B}v_i, \ldots, \mathcal{B}^{m_i-1}v_i\rangle$, con $\mathcal{B}^{m_i}v_i = 0$. Deseamos efectuar la inducción respecto a la dimensión del espacio. Supongamos, que la afirmación del teorema ha sido demostrada para todos los pares $(V', \mathcal{B}')$, donde $\dim V' < \dim V$ y $\mathcal{B}'$ es un operador nilpotente en V'.

Sean, $\mathcal{B}^m = 0$, $\mathcal{B}^{m-1}u \neq 0$. Introduzcamos el subespacio cíclico $U = \langle u, \mathcal{B}u, \ldots, \mathcal{B}^{m-1}u\rangle$ y el espacio cociente $\bar{V} = V/U$, en el que obligamos a actuar al operador cociente $\bar{\mathcal{B}}$: $\bar{\mathcal{B}}\bar{v} = \overline{\mathcal{B}v}$. Aquí $\bar{v} = v + U$ es una clase adjunta con representante v. Como $\bar{\mathcal{B}}^m\bar{v} = \overline{\mathcal{B}^m v} = 0$, entonces, $\bar{\mathcal{B}}$ es un operador nilpotente de índice de nilpotencia $\bar{m} \leqslant m$. Con otras palabras, $\mathcal{B}^{\bar{m}-1}V \not\subseteq U$, $\mathcal{B}^{\bar{m}}V \subseteq U$.

Como $\dim \bar{V} < \dim V$, entonces, por presupuesto de la inducción,

$$\bar{V} = \bar{U}_1 \oplus \ldots \oplus \bar{U}_{s-1}, \quad \bar{U}_i = P[\bar{\mathcal{B}}]\bar{u}_i.$$

Para V obtenemos la descomposición

$$V = U_1 \oplus \ldots \oplus U_{s-1} \oplus U, \tag{4}$$

donde

$$U_i = \langle u_i, \mathcal{B}u_i, \ldots, \mathcal{B}^{m_i-1}u_i\rangle, \quad \mathcal{B}^{m_i}u_i \in U, \quad m_i \leqslant \bar{m} \leqslant m.$$

Los subespacios U_i no son $\mathcal{B}$-invariantes, por cuanto, hablando en general, $\mathcal{B}^{m_i} u_i \neq 0$.

Para mayor comodidad, para i fijando hagamos $w = u_i$, $l = m_i$, $W = U_i = \langle w, \mathcal{B}w, \ldots, B^{l-1}w\rangle$. Por condición,

$$\mathscr{B}^l w = \alpha_k \mathscr{B}^k u + \alpha_{k+1} \mathscr{B}^{k+1} u + \ldots + \alpha_{m-1} \mathscr{B}^{m-1} u, \quad \alpha_k \neq 0$$

(si todos los $\alpha_j = 0$, no tenemos nada que hacer). Aplicando el operador $\mathscr{B}^{m-1-k}$ a la última relación, obtenemos $\mathscr{B}^{m-1-k+l} w = \alpha_k \mathscr{B}^{m-1} u \neq 0$. Como $\mathscr{B}^m = 0$, entonces, esto es posible sólo cuando $l \leqslant k \leqslant m-1$. Haciendo

$$v = w - \alpha_k \mathscr{B}^{k-l} u - \alpha_{k+1} \mathscr{B}^{k-l+1} u - \ldots - \alpha_{m-1} \mathscr{B}^{m-1-l} u,$$

descubrimos, que $\mathscr{B}^{l-1} v = \mathscr{B}^{l-1} w + u' \neq 0$, pero

$$\mathscr{B}^l v = \mathscr{B}^l w - \alpha_k \mathscr{B}^k u - \ldots - \alpha_{m-1} \mathscr{B}^{m-1} u = 0.$$

El espacio cíclico $\langle v, \mathscr{B}v, \ldots, \mathscr{B}^{l-1} v\rangle$ con $\mathscr{B}^l v = 0$ engendra, junto con U, el subespacio $U_i \oplus U$.

Estos razonamientos son legítimos para cualquier i, $1 \leqslant i \leqslant s-1$, por eso, en la descomposición (4), podemos sustituir cada subespacio U_i por $V_i = \langle v_i, \mathscr{B}v_i, \ldots, \mathscr{B}^{m_i-1} v_i\rangle$, $\mathscr{B}v_i = 0$. Haciendo también $v_s = u$, $m_s = m$, $V_s = U$, obtendremos la descomposición

$$V = V_1 \oplus \ldots \oplus V_s,$$

que posee todas las propiedades necesarias.

4. Pasando a la demostración de la unicidad, indiquemos al mismo tiempo la *regla práctica para la reducción de la matriz arbitraria A de orden n a la forma normal de Jordan.*

Para esto es necesario saber hallar el número $N(m, \lambda)$ de células de Jordan $J_{m,\lambda}$ de orden m, que responden al valor propio λ de la matriz A. Comparemos, de un modo habitual, a la matriz A, el operador $\mathscr{A}$, que actúa en el espacio vectorial n-dimensional V, y descompongamos V en la suma directa

$$V = V(\lambda) \oplus V', \tag{5}$$

donde

$$V(\lambda) = \bigoplus_{j=1}^{s} \langle v_j, (\mathscr{A} - \lambda\mathscr{E}) v_j, \ldots, (\mathscr{A} - \lambda\mathscr{E})^{m_j-1} v_j\rangle, \quad V' = \sum_{\lambda' \neq \lambda} V(\lambda').$$

Calcularemos el rango $r_t = \operatorname{rank}(A - \lambda E)^t$ de la matriz $(A - \lambda E)^t$, o, lo que es igual, la dimensión del espacio $(\mathscr{A} - \lambda\mathscr{E})^t V$. Esta dimensión, por supuesto, no depende de la elección de la base en V. Cada uno de los espacios en la descomposición (5) es invariante con

respecto a $(\mathcal{A} - \lambda\mathcal{E})^t$, por eso

$$\dim (\mathcal{A} - \lambda\mathcal{E})^t V = \sum \dim (\mathcal{A} - \lambda\mathcal{E})^t C[\mathcal{A}] v_j + \dim (\mathcal{A} - \lambda\mathcal{E})^t V'.$$

Consideramos, para mayor precisión, $m_1 \leqslant m_2 \leqslant \ldots \leqslant m_s$. Si $m_j \leqslant t$, entonces, $(\mathcal{A} - \lambda\mathcal{E})^t C[\mathcal{A}] v_j = 0$. Para $m_j > t$, tenemos

$$(\mathcal{A} - \lambda\mathcal{E})^t C[\mathcal{A}] v_j = \langle (\mathcal{A} - \lambda\mathcal{E})^t v_j, (\mathcal{A} - \lambda\mathcal{E})^{t+1} v_j, \ldots \\ \ldots (\mathcal{A} - \lambda\mathcal{E})^{m_j-1} v_j \rangle,$$

así que $\dim (\mathcal{A} - \lambda\mathcal{E})^t C[\mathcal{A}] v_j = m_j - t$. En V' el operador $\mathcal{A} - \lambda\mathcal{E}$ no está degenerado (teorema 1), por eso, $\dim (\mathcal{A} - \lambda\mathcal{E})^t V' = \dim V'$. Obtenemos

$$r_t = \sum_{m_j > t} (m_j - t) + \dim V',$$

de donde,

$$\begin{aligned} r_t - r_{t+1} &= \sum_{m_j > t} (m_j - t) - \sum_{m_j > t+1} (m_j - t - 1) = \\ &= \sum_{m_j > t} (m_j - t) - \sum_{m_j > t+1} (m_j - t) + \sum_{m_j > t+1} 1 = \\ &= \sum_{m_j = t+1} 1 + \sum_{m_j > t+1} 1 = N(t+1, \lambda) + N(t+2, \lambda) + \ldots \end{aligned}$$

Por lo tanto, $r_{m-1} - r_m - (r_m - r_{m+1}) = \{N(m, \lambda) + N(m+1, \lambda) + \ldots\} - \{N(m+1, \lambda) + N(m+2, \lambda) + \ldots\} = N(m, \lambda)$, y obtenemos la fórmula definitiva

$$N(m, \lambda) = r_{m-1} - 2r_m + r_{m+1}, \qquad (6)$$
$$m \geqslant 1, \quad r_t = \operatorname{rank} (A - \lambda E)^t, \quad r_0 = n.$$

Observemos, que r_t es una variante de la matriz A (o sea, un número, definido por la clase de semejanza de la matriz A). Esto significa que la *fórmula* (6) *también establece la unicidad de la forma de Jordan* $J(A)$.

Hasta ahora, sobre la matriz C, que cumple la semejanza

$$J(A) = C^{-1}AC,$$

no se ha dicho nada. Pero como ahora A y $J(A)$ son matrices que conocemos, entonces, $C = (c_{ij})$ puede ser hallada del sistema homogé-

neo de ecuaciones lineales

$$CJ(A) - AC = 0$$

de orden n^2. Sea $C_1, \ldots, C_r$, su sistema fundamental de soluciones. Hablando en general, no todas las C_i son matrices no degeneradas, pero, como la forma normal de Jordan $J(A)$ existe, entonces, det $(t_1C_1 + \ldots + t_rC_r) \neq 0$ con coeficientes indeterminados $t_1, \ldots, t_r$, y se pueden elegir $\alpha_1, \ldots, \alpha_r \in \mathbf{C}$, para los cuales det $(\alpha_1C_1 + \ldots$ $\ldots + \alpha_rC_r) \neq 0$. Entonces, $C = \alpha_1C_1 + \ldots + \alpha_rC_r$ es la matriz buscada. Por supuesto, C está lejos de ser unívocamente determinada, incluso con la normación det $C = 1$.

INDICE DE MATERIAS

A nuestros lectores:

Mir edita libros soviéticos traducidos al español, inglés, francés, árabe y otros idiomas extranjeros. Entre ellos figuran las mejores obras de las distintas ramas de la ciencia y la técnica: manuales para los centros de enseñanza superior y escuelas tecnológicas; literatura sobre ciencias naturales y médicas. También se incluyen monografías, libros de divulgación científica y ciencia-ficción. Dirijan sus opiniones a la Editorial Mir, 1 Rizhski per., 2, 129820, Moscú, I-110, GSP, URSS.

Para todos aquellos que desean ampliar
sus conocimientos en Matemáticas la editorial "Mir" propone
las siguientes obras:

Berman G. y otros.
PROBLEMAS Y EJERCICIOS DE ANALISIS MATEMÁTICO

Dankó P., Popov A., Kozhévnicova T.
MATEMÁTICAS SUPERIORES EN EJERCICIOS Y PROBLEMAS.
En dos partes

Efímov A., Demidóvich B.
PROBLEMAS DE MATEMÁTICA PARA LOS CENTROS
DE ENSEÑANZA TÉCNICA SUPERIOR. En dos partes

Kudriávtsev L.
CURSO DE ANÁLISIS MATEMÁTICO. En dos tomos

Lidski V. y otros.
PROBLEMAS DE MATEMATICAS ELEMENTALES

Kurosch A.
ECUACIONES ALGEBRAICAS DE GRADOS ARBITRARIOS